cristie software

CBMR

Cristie Bare Machine Recovery

User Guide

For Windows

May 2014

Version 7.1

Cristie Software Ltd.
New Mill
Chestnut Lane
Stroud GL5 3EH
United Kingdom
Tel:+44(0)1453 847000
Fax:+44(0)1453 847001
cbmr@cristie.com

Cristie Data Products GmbH
Nordring 53-55

63843 Niedernberg
Germany
Tel: +49 (0) 60 28/97 95-0
Fax: +49 (0) 60 28/97 95 7-99
cbmr@cristie.de

Cristie Nordic AB
Gamla Värmdövägen 4

SE-131 37 Nacka
Sweden
Tel:+46(0)8 718 43 30
Fax:+46(0)8 718 53 40
cbmr@cristie.se

Copyright © 1998-2014 Cristie Software Ltd.
All rights reserved.

The software contains proprietary information of Cristie Software Ltd.; it is provided under a license agreement containing restrictions on use and disclosure and is also protected by copyright law. Reverse engineering of the software is prohibited.

Due to continued product development this information may change without notice. The information and intellectual property contained herein is confidential between Cristie Software Ltd. and the client and remains the exclusive property of Cristie Software Ltd. If you find any problems in the documentation, please report them to us in writing. Cristie Software Ltd. does not warrant that this document is error-free.

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the prior written permission of Cristie Software Ltd.

IBM Tivoli Storage Manager (TSM), AIX and TIVOLI are trademarks of the IBM Corporation.

NetWorker and Avamar are trademarks of the EMC Corporation.

Simpana is a trademark of CommVault Inc.

vSphere, vCenter and vCloud are trademarks of VMware Inc.

Hyper-V is a trademark of Microsoft Corporation.

Cristie Management Console (CMC), PC-BaX, UBax, Cristie Storage Manager (CSM), SDB, ABMR (Bare Machine Recovery for EMC Avamar), NBMR (Bare Machine Recovery for EMC NetWorker), SBMR (Bare Machine Recovery for CommVault Simpana), TBMR (Bare Machine Recovery for TSM), CBMR (Cristie Bare Machine Recovery), Recovery Simulator (RS), CloneManager and CRISP (Cristie Recovery ISO Producer) are all trademarks of Cristie Software Ltd.

Cristie Software Ltd
New Mill
Chestnut Lane
Stroud
GL5 3EH
UK

Tel: +44 (0) 1453 847000
Email: cbmr@cristie.com
Website: http://www.cristie.com

Contents

1 Document conventions 8

2 Introduction 9

3 Using CBMR for Disaster Recovery 10

3.1 Preparation ... 10
3.1.1 Create The Bootable Recovery Environment ... 11
3.1.2 TSM Client Version ... 11
3.1.3 Creating a TSM Node ... 11
3.2 The Create Configuration Wizard ... 12
3.2.1 Storing Configuration Parameters ... 13
3.3 Creating and Testing DR Backup ... 14
3.4 Restoring Your System ... 19
3.4.1 Dissimilar Hardware Support ... 20
Hardware Differences ... 20
Current Support ... 21
Using HWWizard and the WinPE2 or WinPE4 Based DR Console ... 21
3.4.2 WinPE2 or WinPE4 based CBMR Recovery Console ... 21
CBMR Recovery Console Main Menu ... 23
Start Automatic Recovery Wizard ... 25
File Restore Type ... 25
TSM Restore Type ... 26
Specify Key Repository ... 28
Confirm Volume Layout ... 29
Select Datasets to Restore ... 33
Clone Settings ... 34
Proceed With The Recovery ... 35
Disk Recovery Sequence ... 36
Disk Scaling ... 38
Dissimilar Hardware ... 39
Start Manual Recovery Sequence ... 41
File Restore Type ... 42
TSM Restore Type ... 43
Specify Key Repository ... 44
Create Partition and Volumes ... 46
Restore Files ... 50
Make Bootable ... 52
Dissimilar Hardware ... 54
Tools ... 55
Cristie Network Configurator Tool ... 57
Configure NIC Parameters ... 58
Assign Static or DHCP IP Settings ... 60
Map a Network Drive ... 61
Disconnect Network Drives ... 62
Setup DNS Servers ... 63

Copyright © 1998-2014 Cristie Software Ltd.

Setup Network Identification ... 64
Display MAC Address ... 65
Dissimilar Hardware Wizard ... 66
Load a Driver ... 72
Show Log and Error Reports ... 73
Copy Log and Error Report Files ... 74
Close Recovery Console and Reboot ... 75

4 CBMR in More Detail 76

4.1 User Interface Overview ... 76
4.1.1 **CBMR Setup Disaster Recovery Configuration ... 77**
4.1.2 **CBMR Run or Schedule Disaster Recovery Backup ... 77**
4.1.3 **View Log Files ... 78**
4.1.4 **CBMR Tools ... 79**
4.1.5 **CBMR Backup Selection Tool ... 79**
4.1.6 **Backup Schedules ... 80**
4.1.7 **Backup Catalogue ... 80**
4.1.8 **Backup Locations ... 81**
4.1.9 **CBMR Default settings window ... 81**
4.1.10 **Directory Tree ... 82**
4.2 Getting Started ... 83
4.2.1 **Configuring CBMR ... 84**
Default Settings ... 84
Backup Properties ... 86
Restore Properties ... 88
Backup Location Properties ... 89
Backup Catalogue Properties ... 91
Log File Properties ... 92
Performance Page ... 93
Exclude Files ... 95
Encryption Properties ... 96
Disaster Recovery Properties Page ... 97
4.2.2 **Configuring Backup Locations ... 98**
New Backup Location ... 99
SCSI/IDE Backup Location Setup ... 101
Virtual Tape Device (VTD) Backup Location ... 102
Cascaded Backup Location Setup ... 102
Robotics/Media Handler Setup ... 103
Library Backup Location Setup and Configuration ... 105
TSM Backup Location Setup ... 107
Set a Default Backup Location ... 110
Viewing and Deleting Locations ... 110
4.2.3 **Setting up CBMR for Routine Operations ... 111**
4.3 Introduction to Backing up data ... 111
4.3.1 **Backup Schedules and Selection Scripts ... 112**
Creating a Backup Schedule ... 112
Common Settings ... 114
Save Backup Selection Script ... 115
Backup Location ... 116
Compression and Encryption ... 117
File Access ... 118
Logging and Backup Catalogue ... 119
Backup Wizard - Data To Backup ... 120

Copyright © 1998-2014 Cristie Software Ltd.

System State ... 122
Selecting Network Shares ... 122
Set Attach Info ... 123
File Selection List ... 123
Selecting Network Shares or Volumes ... 124
Logon Failure ... 125
Applying File Restrictions ... 126
Viewing and Modifying Existing Backup Selection Scripts ... 127
Backup Selection Script Editor ... 128
Backup Options Page ... 128
Backup Compression and Encryption ... 130
Script Name ... 130
Media Header Overview ... 130
Deleting a Backup Selection Script ... 130
Script Properties ... 131
Running a Backup Using an Existing Selection Script ... 131
4.3.2 **Dataset Settings** ... **131**
Dataset Details ... 131
Estimate Backup Size ... 132
4.3.3 **Specifying a Backup Catalogue Entry** ... **132**
4.3.4 **CBMR Log Files Overview** ... **133**
Managing Log Files ... 133
Viewing and Deleting Log Files ... 134
4.3.5 **Backup Encryption** ... **134**
The Key Repository File ... 134
Passphrases and Encryption Keys ... 135
Restoring Encrypted Backups ... 136
Encryption Algorithms ... 137
4.3.6 **Start Backup** ... **137**
4.3.7 **Aborting Backup** ... **139**
4.3.8 **Verify and Compare** ... **139**
Programs ... 140
Dialogue ... 141
4.3.9 **Statistics Report** ... **141**
4.4 Restoring Files ... **141**
4.4.1 **Restore/Compare/Verify Wizard** ... **142**
Data Source ... 143
Catalogue Volume ... 144
Select Data ... 144
Select Location ... 145
Restore Options ... 145
Logfile Options ... 146
Finished ... 146
4.4.2 **Restoring From the Backup Catalogue** ... **147**
4.4.3 **Browse Backup Location** ... **147**
Options (Restore/Compare/Verify) ... 148
4.4.4 **Redirecting Files** ... **149**
Redirection Dialogue ... 149
Redirection List ... 150
4.5 Windows Registry ... **150**
4.5.1 **Structure of the Registry** ... **150**
4.5.2 **How is it backed up?** ... **151**
4.5.3 **Restoring** ... **151**
4.6 Scheduler Overview ... **151**

Copyright © 1998-2014 Cristie Software Ltd.

4.6.1 **Operating the Scheduler** ... **152**
4.6.2 **Creating a New Scheduled Job** ... **152**
Program Title ... 153
Program ... 153
Set Date and Time ... 154
Scheduler Options ... 154
4.6.3 **Scheduled Task Wizard** ... **155**
Schedule ... 156
Task ... 158
Finished ... 159
4.6.4 **Managing Scheduler Jobs** ... **159**
4.6.5 **System Dependent Information** ... **160**
4.6.6 **Using Batch Files** ... **161**
4.7 Backup Catalogue ... **161**
4.7.1 **Viewing the Catalogue Contents** ... **162**
4.7.2 **Information Stored about the Backup** ... **162**
Media Header ... 162
Dataset Header ... 164
4.7.3 **Browse Backup Catalogue** ... **165**
4.7.4 **Modifying the Level of Catalogue Information** ... **166**
4.7.5 **Creating a New Catalogue Volume** ... **166**
4.7.6 **Deleting, Searching and Restoring** ... **167**
4.7.7 **Backup Location Search** ... **167**
4.7.8 **Select Backup Location To Use** ... **168**
4.7.9 **Options (Restore/Compare/Verify)** ... **169**
4.8 Backup Strategy ... **170**
4.8.1 **Example Routines** ... **171**
4.9 Running CBMR from the Command-line ... **172**
4.9.1 **PC-BaX Command Line Options** ... **173**
4.9.2 **CBMRwin.exe Command Line Options** ... **174**
4.9.3 **CBMRCfg.exe Command Line Options** ... **175**
4.9.4 **CBMR Configuration Files** ... **175**
PCBAX.INI ... 175
CBM.INI ... 175
USERSHAR.INI ... 176
USERINFO.INI ... 176
DTEXC.INI ... 176
KEYREPOSITORY.INI ... 176
4.10 Media Utilities ... **176**
4.10.1 **Media Management** ... **176**
4.10.2 **Read Header** ... **177**
4.10.3 **Retension** ... **177**
4.10.4 **Unload** ... **177**
4.10.5 **Create New Header** ... **178**
4.10.6 **New Media Header** ... **178**
4.10.7 **Security Erase** ... **178**
4.10.8 **Initialise** ... **178**
4.10.9 **Library Control Panel** ... **178**

5 Appendicies 180

5.1 Windows 8 Storage Space and 2012 Storage Pool Support ... **180**
5.2 uEFI and MBR BIOS support ... **180**

Copyright © 1998-2014 Cristie Software Ltd.

6 Support 182

6.1 Online Help 182
6.2 Technical Support 182

7 Glossary of Terms 184

Copyright © 1998-2014 Cristie Software Ltd.

1 Document conventions

The following typographical conventions are used throughout this guide:

`/etc/passwd`	represents command-line commands, options, parameters, directory names and filenames
Next >	used to signify clickable buttons on a GUI dialogue
Note:	describes something of importance related to the current topic

2 Introduction

CBMR provides complete data protection, as well as the ability to recover critical servers from scratch within minutes. CBMR can be used as a standalone backup product and provides an ideal solution for server migration.

CBMR backs up the operating system and hard disk configuration of critical servers, enabling rapid recovery of data to an identical state following damage to or failure of the physical hardware, or a corruption of the operating system.

Please refer to the supplied **Readme** document for a list of supported Windows OS's.

CBMR also provides the ability to clone to a new machine from an existing backup. The cloning option allows the hostname and/or the IP address to be changed during the recovery.

CBMR is available as a single edition suitable for all platform types. You must have one of the supported Windows™ Operating Systems correctly installed prior to proceeding with the installation of CBMR.

A low cost licensed version of CBMR is also available. This edition offers exactly the same functionality as the full Server version, but supports Windows desktop OS's only.

To minimise the impact of a system failure, you need to have a restore strategy in place. CBMR allows you to recover Windows Workstations and Servers without first having to re-install the operating system or backup software. This reduces the recovery time significantly. All you need is disaster recovery media from which to boot your computer and a disaster recovery backup of the original Windows system.

Finally, a full backup of the system can be restored using the backup features of CBMR or any other preferred third party Backup/Restore software.

Backups can be performed to a variety of different Backup Locations and media, including IBM's Tivoli Storage Manager, tape, disk, network-attached storage etc.

IMPORTANT: Refer to the installed Readme file for any limitations and last minute updates.

Copyright © 1998-2014 Cristie Software Ltd.

3 Using CBMR for Disaster Recovery

This section describes the essential elements of CBMR when used for Disaster Recovery.

If you wish to use CBMR in standard backup/recovery mode please refer to section CBMR in More Detail.

CBMR can protect a system against disaster all the time, if set up and configured correctly. The following sections explain this procedure.

3.1 Preparation

To use CBMR in a production environment for DR purposes, you must follow the procedure in the order listed below:

1. **Installation** (refer to the **CBMR Installation and Licensing Guide**)
   - *Install the CBMR Backup and Restore software*
   - *License the Software (using a Trial or Full license)*

2. **Prepare WinPE2 or WinPE4 DR ISO/CD-ROM** (refer to the **Cristie Recovery ISO Producer User Guide**)
   - *Install and run the Cristie Recovery ISO Producer (CRISP) tool on a suitable system to create the CBMR WinPE2 or WinPE4 based DR environment in ISO form. The ISO may then be burnt to CD or DVD physical media if required. This only needs to be done once.*

3. **Machine Configuration**
   - *Save the Machine Configuration parameters. Update when significant hardware changes are made. Configuration parameters are always saved into the backup itself (this cannot be changed).*

4. **Backup system (OS) and User data**
   - *Perform regular Disaster Recovery backups as required*
   - *Perform any extra standard data backups as required*

You will then be ready to Restore the system from the Disaster Recovery Backup in conjunction with the DR media when required.

> ***Note if using TSM, check the TSM BA Client version in use on your server. Also Create a TSM Client Node.***

To perform a Bare Machine Recovery you must:

1. *Boot into the DR environment on the machine to be restored from the CBMR WinPE2 or WinPE4 DR CD or DVD.*
2. *Perform a system recovery from the specified backup location.*

3. Perform conventional data recovery from your third party backups if necessary.

3.1.1 Create The Bootable Recovery Environment

The supplied CRISP tool is used to create the CBMR recovery environment. This environment is based upon a customised version of Microsoft's WinPE2 or WinPE4.

Once created the recovery environment is booted on the target system and then drives the restore process.

This tool should be run in conjunction with the supplied CRISP WinPE2 or WinPE4 Fileset for CBMR 7.1. The fileset should be installed alongside the CRISP on the same host or technician machine.

A full discussion of how to install and run CRISP is contained in the separate **CRISP User Guide**. Note that the CRISP does not need to be installed on the system to be backed up; any suitable machine will do.

Output from the CRISP tool is a bootable WinPE2 or WinPE4 ISO file which can then be burnt to physical media (CD or DVD) or mounted directly in a VM environment.

This media is then booted on the target machine to control the recovery operation.

3.1.2 TSM Client Version

If you intend to use TSM as your backup location it is important to check the version of the TSM Client installed on your machine. Versions supported by CBMR are summarised in the **Readme** document.

> ***Note: Please refer to the Readme document for the latest client support details.***

If you are not using TSM, please skip this step.

3.1.3 Creating a TSM Node

This step is only required if TSM is used in the recovery procedure. Please ignore this step if TSM is not being used.

CBMR will connect to a TSM server as a client node. The machine's operating system files and other important files will be stored under a Filespace in the client node. If you need to create a Client node using the TSM Admin Client, refer to the **TSM Administrator Guide** for further information.

To use the TSM module, you must enable CBMR to backup to the IBM Tivoli Storage Manager by creating a dedicated node via the TSM Admin client.

The settings required for the node are:

Archive Delete Allowed	YES
Backup Delete Allowed	YES
Client Compression setting	CLIENT
Force password reset	NO

Copyright © 1998-2014 Cristie Software Ltd.

Node Type	CLIENT

In addition, you must consider your password policy. If you specify a Password Expiration period, you will have to set the password in CBMR every time the password expires.

> *Note: automatic password generation for the client nodes is supported in CBMR 5 and later.*

Additional Configuration to Maintain Multiple Backup Versions

If it is required to hold more than one version of the DR backup in the same filespace, then the node must be setup correctly to support this.

You must have a **Management Class (MC)**, which contains a **Backup Copy Group (BCG)** and an **Archive Copy Group (ACG)**.Your node needs to be registered to use the **MC**.

The parameters of the **BCG** of interest are:

- Versions Data Exists = 2
- Versions Data Deleted = 1
- Retain Extra Versions = 30
- Retain Only Version = 60

In this example, there can be two versions of an object. The Versions Data Deleted attribute specifies the maximum number of different backup versions (1 in this case) retained for files and directories that you erased from your file system. This parameter is ignored as long as the file or directory remains in your file system.

The expiration date for the remaining versions is based on the retain extra versions and retain only version parameters. In the example, if there is more than one version and one is deleted, the deleted one will be kept for 30 days. The only remaining copy of the object will be retained for 60 days (that is AFTER you make it inactive).

> *Note: if several versions of a DR backup are maintained in TSM, the WinPE2 or WinPE4 recovery environment will allow you to choose a specific version to restore.*

3.2 The Create Configuration Wizard

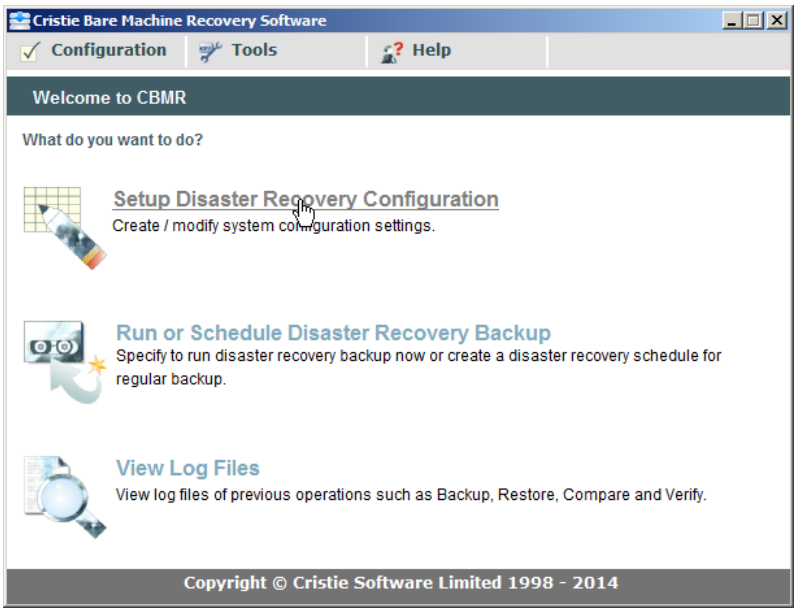
Configuration information can be stored only within the DR backup itself.

As part of this process, the details about hard disks, operating system, storage controller(s), network adapter(s) and network settings are stored. You can override some of these details if you wish.

The next section discusses this in detail.

3.2.1 Storing Configuration Parameters

In the CBMR main window, click on **Setup Disaster Recovery Configuration**:

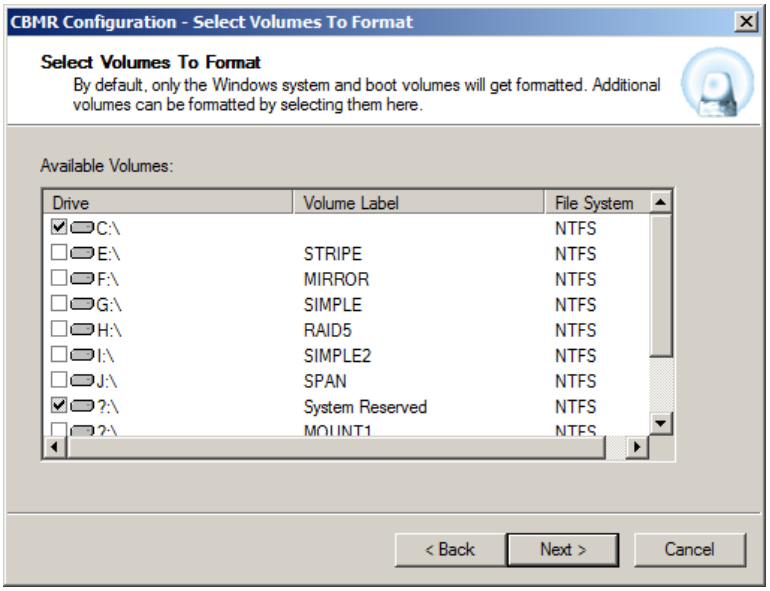

Cristie Bare Machine Recovery Software
Configuration
Tools
Help
Welcome to CBMR
What do you want to do?
Setup Disaster Recovery Configuration
Create / modify system configuration settings.
Run or Schedule Disaster Recovery Backup
Specify to run disaster recovery backup now or create a disaster recovery schedule for regular backup.
View Log Files
View log files of previous operations such as Backup, Restore, Compare and Verify.
Copyright © Cristie Software Limited 1998 - 2014

The **CBMR Configuration - Welcome** dialogue will appear.

CBMR Configuration - Welcome
Welcome to Disaster Recovery configuration wizard
This wizard will take you through the steps in configuring CBMR for recovery on this system.
Select the [Next] button to continue.
< Back
Next >
Cancel

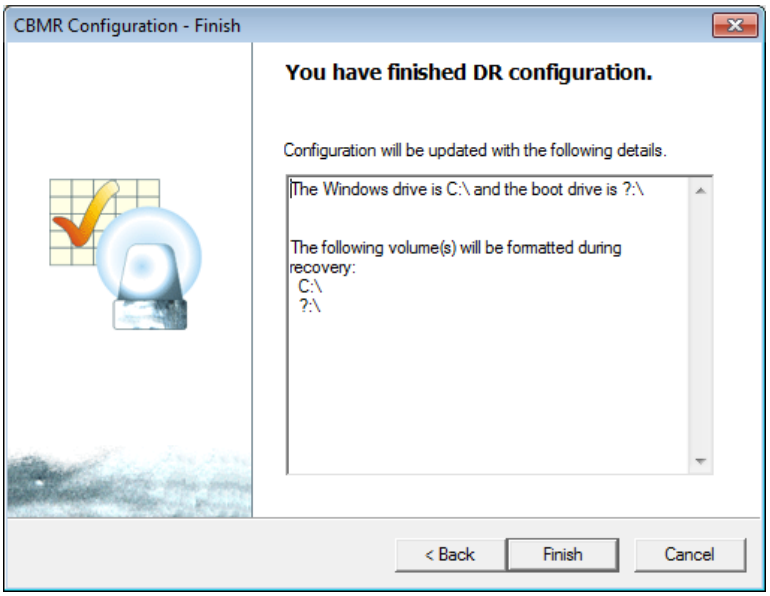
Select Next> and the **CBMR Configuration - Select Volumes to Format** dialogue will help you to select the disks and partitions which should be formatted during a recovery:

Copyright © 1998-2014 Cristie Software Ltd.


CBMR Configuration - Select Volumes To Format
Select Volumes To Format
By default, only the Windows system and boot volumes will get formatted. Additional volumes can be formatted by selecting them here.
Available Volumes:
Drive
Volume Label
File System
C:\ NTFS
E:\ STRIPE NTFS
F:\ MIRROR NTFS
G:\ SIMPLE NTFS
H:\ RAID5 NTFS
I:\ SIMPLE2 NTFS
J:\ SPAN NTFS
?:\ System Reserved NTFS
< Back
Next >
Cancel

The Windows boot and system partitions will be selected by default and you cannot exclude them. All other volumes and partitions can be selected or de-selected by clicking on the selection box which toggles the current selection.

Click on Next> to confirm the disks/partitions for formatting.


CBMR Configuration - Finish
You have finished DR configuration.
Configuration will be updated with the following details.
The Windows drive is C:\ and the boot drive is ?:\
The following volume(s) will be formatted during recovery:
C:\
?:\
< Back
Finish
Cancel

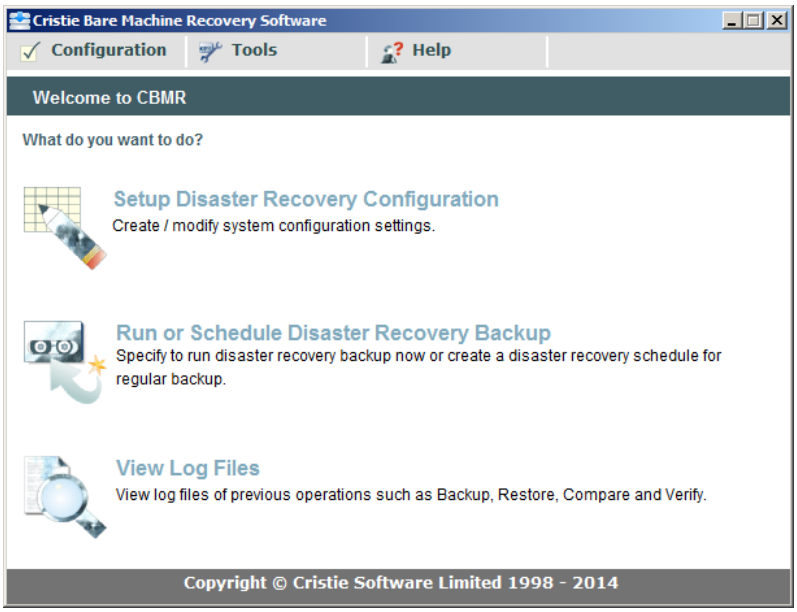
Check that all your selections are correct. If you need to modify any of these settings, choose the <Back button and modify your selection.

Finally, click Finish to save the settings. When a DR backup is run, the configuration information will be stored to a folder **CBMRCFG** on the Windows drive. This folder will be automatically included with the backup. This folder should never be removed manually, nor its attributes or contents changed.

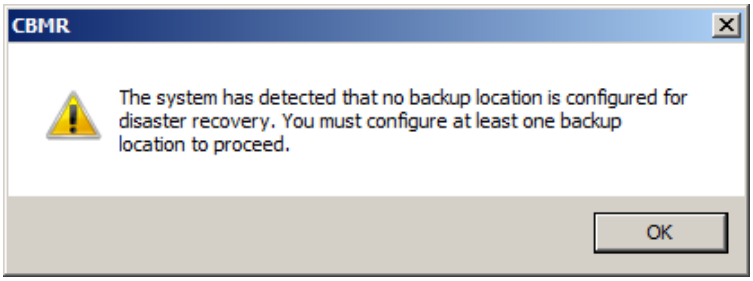
3.3 Creating and Testing DR Backup

For locally attached physical Backup Locations (ie tape, library auto-loader or local disk), insert a clean tape in the tape drive or ensure there is enough space on the backup disk.

Click on the **Run or Schedule Disaster Recovery Backup** option in the CBMR main window:

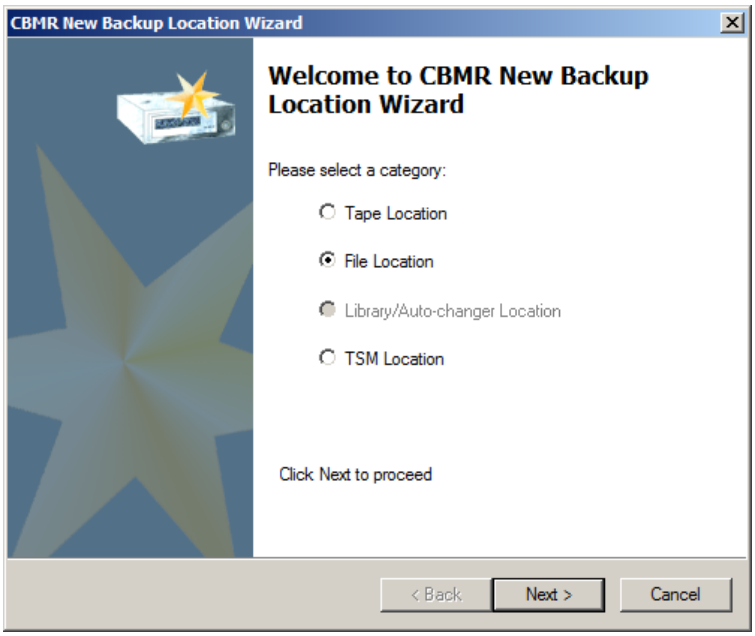

Cristie Bare Machine Recovery Software
Configuration
Tools
Help
Welcome to CBMR
What do you want to do?
Setup Disaster Recovery Configuration
Create / modify system configuration settings.
Run or Schedule Disaster Recovery Backup
Specify to run disaster recovery backup now or create a disaster recovery schedule for regular backup.
View Log Files
View log files of previous operations such as Backup, Restore, Compare and Verify.
Copyright © Cristie Software Limited 1998 - 2014

At least one Backup location must exist in order to proceed through the wizard. If none have been previously configured, you will see a message that indicates this.


CBMR
The system has detected that no backup location is configured for disaster recovery. You must configure at least one backup location to proceed.
OK

Click OK to accept the message.

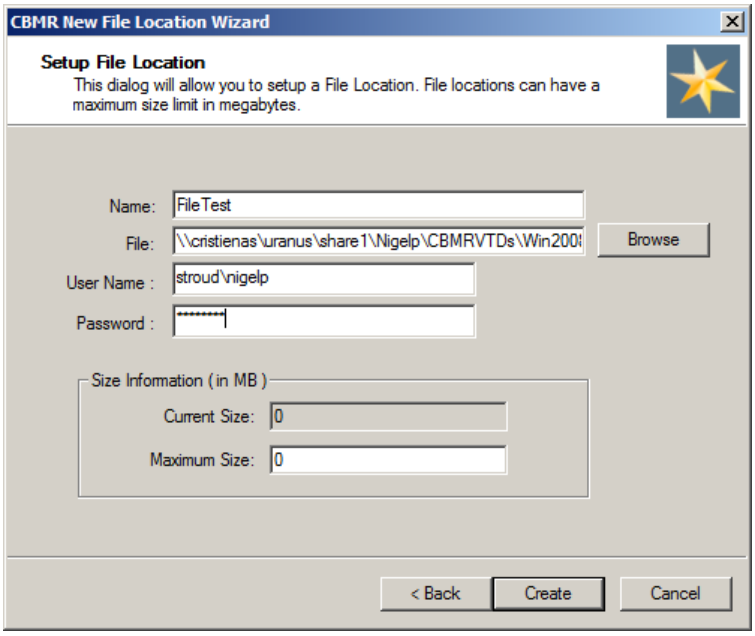
This will open the **CBMR - New Backup Location Wizard** welcome dialogue.



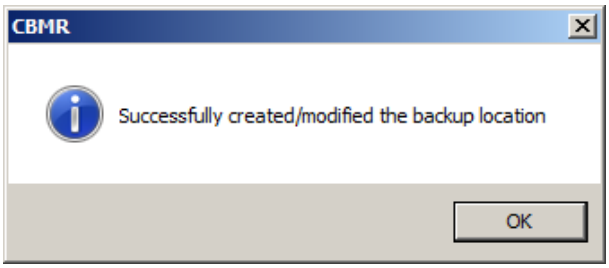
Copyright © 1998-2014 Cristie Software Ltd.

Select the Category of Backup required, for example, File.

Select Next> to continue and the **CBMR - New File Location Wizard** is displayed:



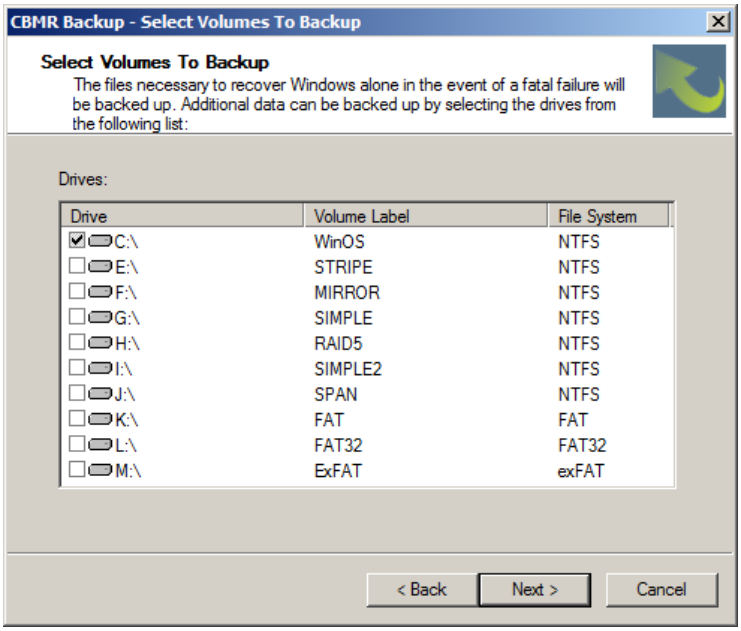
Click Create to create the specified File Location. This is confirmed thus:



On clicking OK to continue and the following dialogue is displayed:

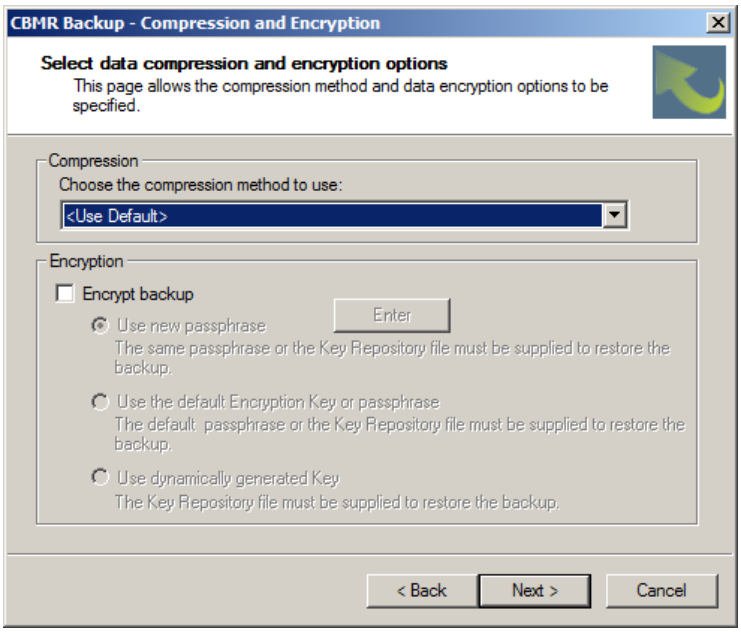
CBMR Backup - Welcome
Welcome to Disaster Recovery Backup Wizard.
These pages will enable you to define a DR Backup. The DR Backup may be run immediately, saved for future use or scheduled to run at regular time.
< Back
Next >
Cancel

Click Next > and the **CBMR Backup - Select Volumes To Backup** dialogue is displayed:


CBMR Backup - Select Volumes To Backup
Select Volumes To Backup
The files necessary to recover Windows alone in the event of a fatal failure will be backed up. Additional data can be backed up by selecting the drives from the following list:
Drives:
Drive
Volume Label
File System
C:\ WinOS NTFS
E:\ STRIPE NTFS
F:\ MIRROR NTFS
G:\ SIMPLE NTFS
H:\ RAID5 NTFS
I:\ SIMPLE2 NTFS
J:\ SPAN NTFS
K:\ FAT FAT
L:\ FAT32 FAT32
M:\ ExFAT exFAT
< Back
Next >
Cancel

The dialogue shows all the available hard disk drives (including any partitions mounted on folders). You can select all or a sub-set as required. Whatever you choose, the Windows folder, the TSM installation folder (if installed), the Registry, "Documents and Settings" folder and CBMR folder will *always* get backed up.

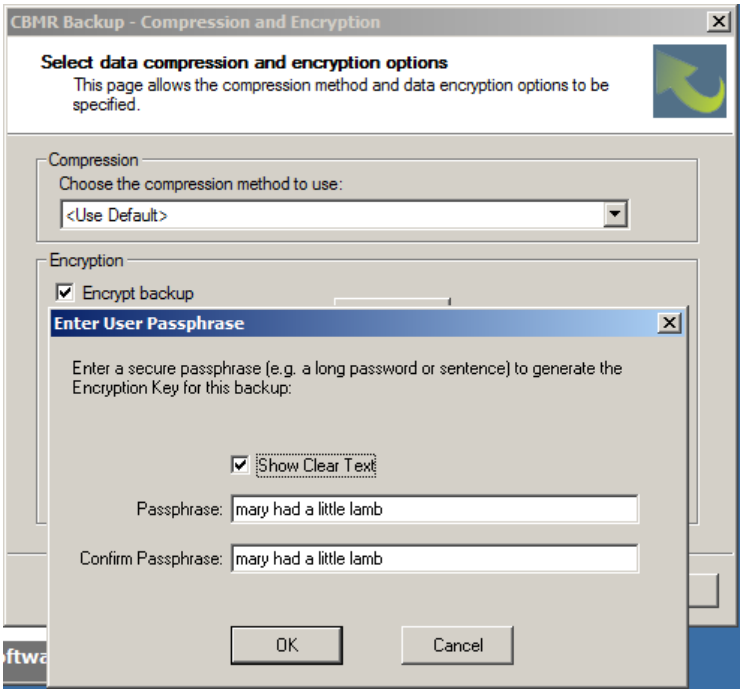
Select Next> to open the **CBMR Backup - Compression and Encryption Options** dialogue:


CBMR Backup - Compression and Encryption
Select data compression and encryption options
This page allows the compression method and data encryption options to be specified.
Compression
Choose the compression method to use:
<Use Default>
Encryption
Encrypt backup
Enter
Use new passphrase
The same passphrase or the Key Repository file must be supplied to restore the backup.
Use the default Encryption Key or passphrase
The default passphrase or the Key Repository file must be supplied to restore the backup.
Use dynamically generated Key
The Key Repository file must be supplied to restore the backup.
< Back
Next >
Cancel

Select <**Use Default**> to accept the default compression method. Alternatives are available via the drop-down menu.

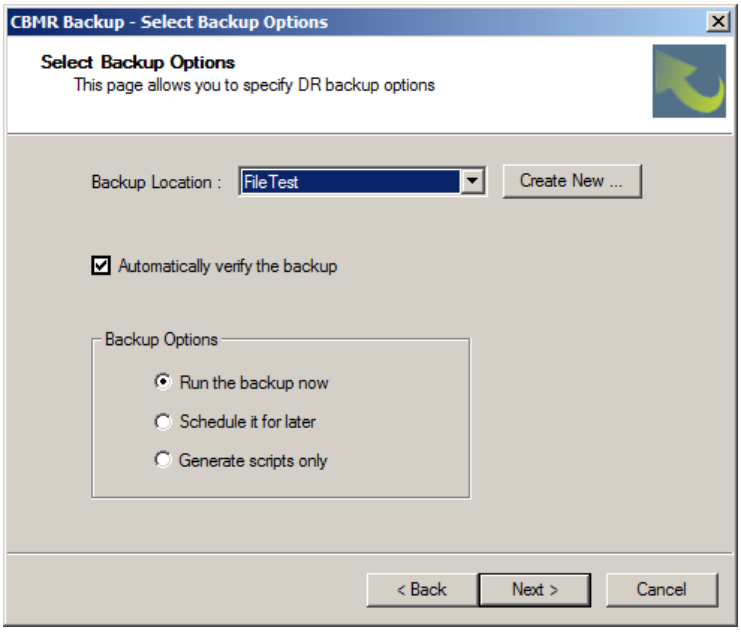
If you wish to encrypt the DR backup, select the **Encrypt backup** tick-box.

Copyright © 1998-2014 Cristie Software Ltd.


CBMR Backup - Compression and Encryption
Select data compression and encryption options
This page allows the compression method and data encryption options to be specified.
Compression
Choose the compression method to use:
<Use Default>
Encryption
Encrypt backup
Enter User Passphrase
Enter a secure passphrase (e.g. a long password or sentence) to generate the Encryption Key for this backup:
Show Clear Text
Passphrase:
mary had a little lamb
Confirm Passphrase:
mary had a little lamb
OK
Cancel

Use either the system default key or enter a new passphrase or key. Click OK.

Select Next> to display the **CBMR Backup - Select Backup Options** dialogue:



The **Automatically verify the backup** check box will be checked by default, which will force an integrity check of the backup after completion. This is independent of the program default settings.

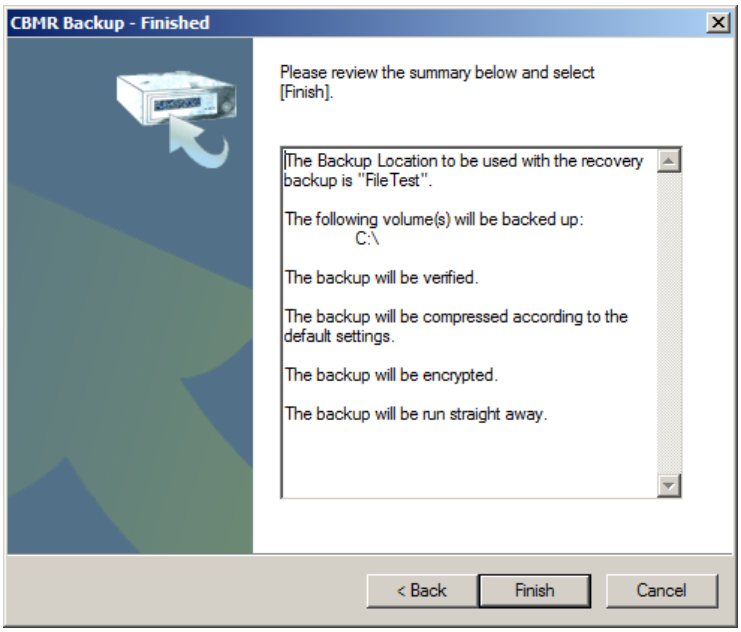
> ***Note: this can be turned off to reduce the overall backup time by clearing the check box. However, this is not recommended.***

Select **Run the backup now** if you wish to run the DR backup immediately on pressing the Next> button.

Select **Schedule it for later** if you wish to schedule it either using the CBMR or Windows Scheduler, depending on the default settings.

Select **Generate scripts only** if you wish to prepare a script (disrec.scp) for scheduling the DR backup. No actual backup will be performed in this case.

Press Next> to continue to the last page of the Wizard.


CBMR Backup - Finished
Please review the summary below and select [Finish].
The Backup Location to be used with the recovery backup is "FileTest".
The following volume(s) will be backed up:
C:\
The backup will be verified.
The backup will be compressed according to the default settings.
The backup will be encrypted.
The backup will be run straight away.
< Back
Finish
Cancel

Select Finish to start the backup process.

> ***Note: it is not possible to run a DR backup until the DR configuration has been setup and saved at least once.***

Testing the Backup Location Using WinPE2 or WinPE4 Mode Recovery

Insert the WinPE2 or WinPE4 Disaster Recovery DVD/CD in your DVD/CD-ROM drive and reboot your computer from the disk. Follow the on-screen instructions and boot the Windows PE Recovery Console.

> ***Note: before storing your Disaster Recovery Disk (and the DR Backup tape if used), it is important to check that the Disaster Recovery works and the Backup Location is accessible. You only need to test that you can connect to the backup data. The description below is a summary of the process which is described in more detail in the section Restoring Your System.***

3.4 Restoring Your System

This section discusses the steps required to run a recover sequence using the CBMR Recovery Console. The console is booted from the media created by CRISP in conjunction with the CRISP WinPE2 or WinPE4 Fileset for CBMR 7.1 (see Create the bootable cloning environment for further details).

The WinPE2 or WinPE4 based recovery environment is booted on the ***target*** system. This could be the original or a dissimilar system.

A typical CBMR recovery sequence consists of the following steps.

1. *Install and run the **Cristie Recovery ISO Producer** (**CRISP**) tool on a suitable system to*

Copyright © 1998-2014 Cristie Software Ltd.

create the CBMR WinPE2 or WinPE4 based recovery environment. This only needs to be done once.

2. *Boot the CBMR WinPE2 or WinPE4 recovery environment on the **target** system.*
3. *Run a restore sequence from the recovery environment on the **target** system using the CBMR backup.*
4. *When the restore operation is complete and, before booting the system, you may change the hostname and IP address as required. If the target system uses different hardware from the source system inject additional drivers into the system using the hardware wizard tool. This tool will detect any new devices in the target system and prompt for the drivers.*
5. *Boot the recovered system.*

3.4.1 Dissimilar Hardware Support

CBMR can restore a Windows system to the same or similar hardware, as well as to hardware with significant changes. The dissimilar restore capability makes CBMR a deployment or server migration tool, as well as a disaster recovery tool. CBMR contains a Dissimilar Hardware (DHW) component that allows new drivers to be injected into recovering systems to accommodate different hardware in the target machine.

> ***Note: it should be kept in mind that Microsoft Windows is a complex operating system which has its own hardware dependencies and limitations.***

This section discusses various issues involved in recovering a Windows server or workstation using CBMR version 7.1 for Windows . The original machine may have been configured for a very different set of hardware to the machine to which you are recovering. The ability to recover to different hardware is becoming an increasingly important feature in any disaster recovery software. This is due to the fact that hardware is superseded very quickly. So it may not be practical to find an exact replacement for a server or a failed component.

Over a period of time, our dissimilar hardware support has evolved and with the latest release, a new Plug-and-Play manager is incorporated which will prompt for the correct driver for the new hardware. With a little knowledge of drivers for motherboard resources, it is also possible to change any aspect of Windows by using the Manual Driver Install option. The rest of the document will explain the steps used in CBMR to recover a Windows system to a different machine.

The WinPE2 or WinPE4 DR environment is now created by the Customer using the Cristie Recovery ISO Producer (CRISP) tool. This tool has the ability to allow Customers to add their own drivers for both WinPE2 or WinPE4 and DHW support. Therefore the Customer is no longer dependent upon the default set of dissimilar hardware drivers provided by Cristie Software Ltd..

3.4.1.1 Hardware Differences

Almost all hardware components can be different in a new system. From the CBMR standpoint, the following are considered different if:

- One or more new hard disks are added or removed from the system
- One or more hard disk is replaced with a bigger or smaller capacity disk
- Network adapters are changed
- Mass Storage Controllers like SCSI/RAID are changed
- Motherboard is different
- One or more CPUs are added or removed. The CPU could also be a different model

3.4.1.2 Current Support

CBMR addresses the different dissimilar hardware scenarios as follows:

- **One or more new hard disks are added or removed from the system**
  If more disks are added, they need to be partitioned and formatted manually using Windows disk management tools

- **One or more hard disk is replaced with a bigger or smaller capacity disk**
  The disks may be scaled up or down in proportion to the original disk layout

- **Network Adapters are changed**
  Drivers will be installed automatically if they are PnP capable

- **Mass Storage Controllers like SCSI/RAID are changed**
  The correct drivers must be installed using the Cristie Dissimilar Hardware Wizard utility, which is run during the WinPE2 or WinPE4 DR sequence. Dissimilar hardware will be automatically detected during the DR process prompting the User to specify the location of the new drivers.

> ***It is the Customer's responsibility to locate the correct drivers for the dissimilar system.***

3.4.1.3 Using HWWizard and the WinPE2 or WinPE4 Based DR Console

The CBMR Dissimilar Hardware Wizard (**DHW**) is a comprehensive utility which will install new files and drivers to a recently restored Windows system. This tool is run from the WinPE2 or WinPE4 Recovery environment *after* you have recovered the file system. It is run as part of the automatic recovery sequence, but may also be run manually if required.

The DHW will also allow 64-bit drivers to be 'injected' into a recovering 64-bit system. Ensure you have the correct drivers for the target system (i.e. 32 or 64-bit).

> ***Note: Drivers for recovering to VMware and Hyper-V are supplied on the recovery CD.***

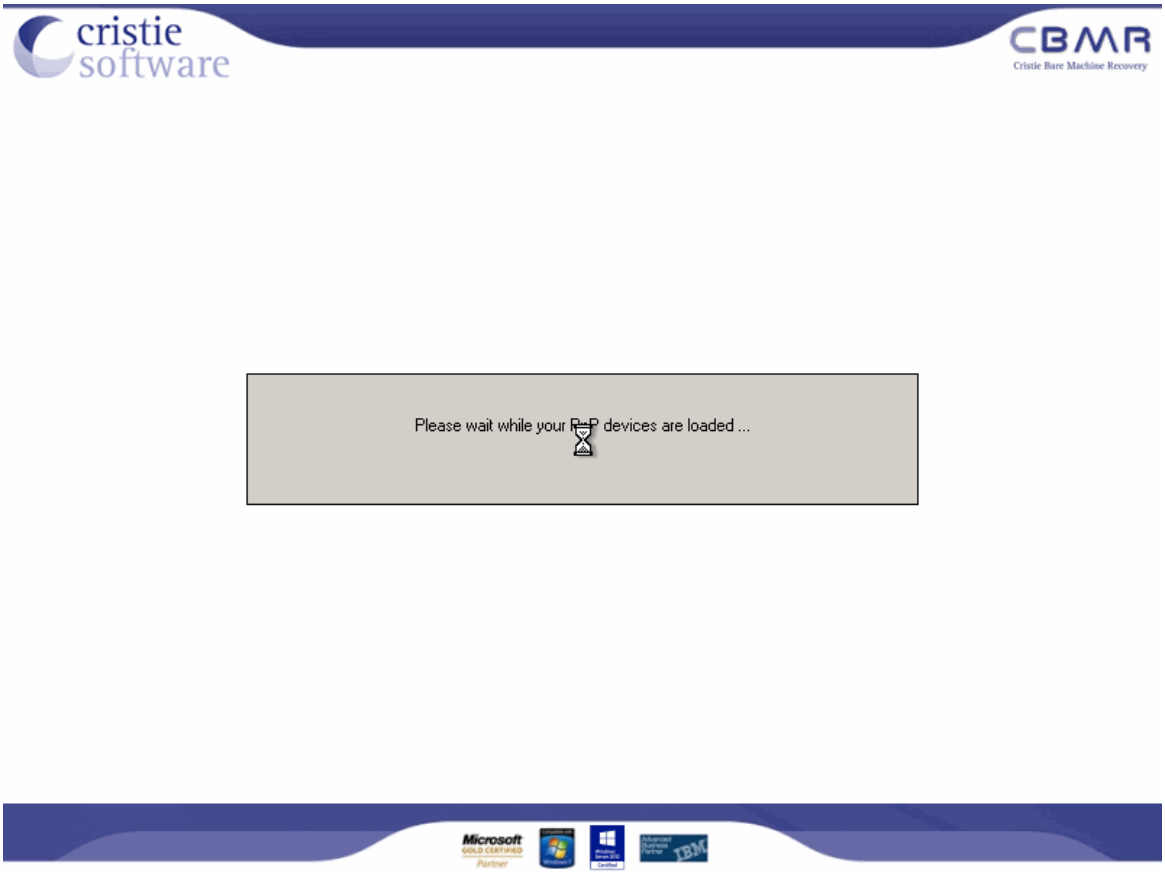
3.4.2 WinPE2 or WinPE4 based CBMR Recovery Console

When the **WinPE2 or WinPE4 CBMR Console** is booted, a Windows installation-like boot procedure is started.

During the boot process, WinPE2 or WinPE4 drivers for your **Plug and Play** devices will be loaded - in particular the **Mass Storage** devices and **Network Adapters**. When the WinPE2 or WinPE4 system has booted, it is possible to remove the CD if you wish.

> ***Note: the DR Console will automatically reboot 72 hours after starting. This is an operating limitation of the MIcrosoft Windows WinPE2 or WinPE4 environment.***

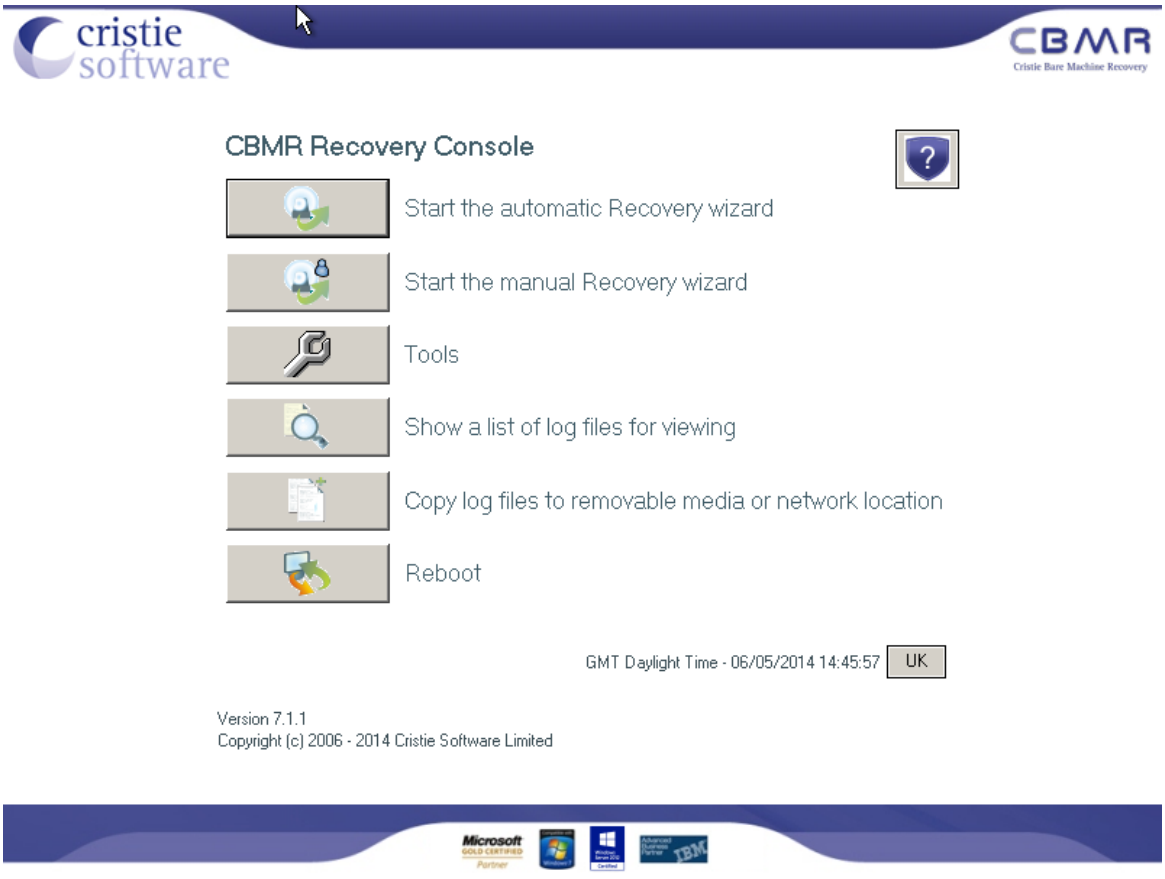
Copyright © 1998-2014 Cristie Software Ltd.



When this sequence completes, the **CBMR Recovery Console** will be shown.

3.4.2.1 CBMR Recovery Console Main Menu

When you boot the **WinPE2 or WinPE4** DR environment (the <%CP_WINPE2%> and <%CP_WINPE4%> versions are very similar), you will see the **CBMR Recovery Console** Main Menu as below:


cristie software
CBMR
Cristie Bare Machine Recovery
CBMR Recovery Console
Start the automatic Recovery wizard
Start the manual Recovery wizard
Tools
Show a list of log files for viewing
Copy log files to removable media or network location
Reboot
GMT Daylight Time - 06/05/2014 14:45:57
UK
Version 7.1.1
Copyright (c) 2006 - 2014 Cristie Software Limited

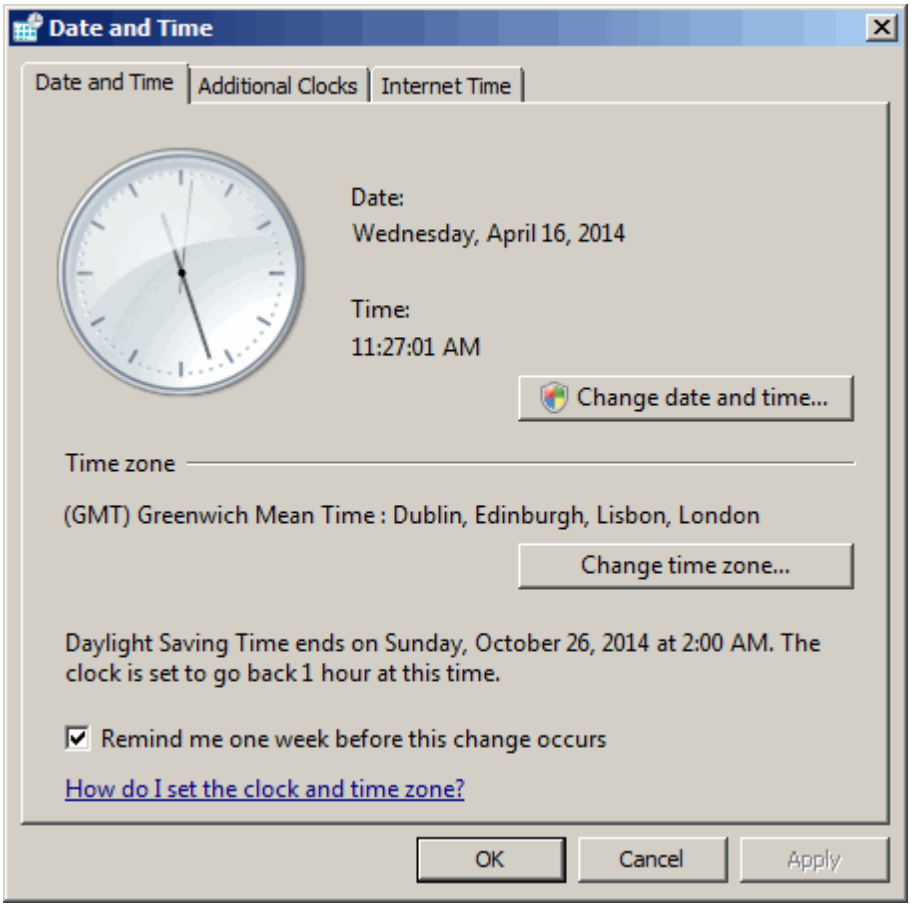
You may configure the format of the displayed date/time and the keyboard layout, by pressing the locale icon. Note this icon will be shown according to the locale of the host system used to create the ISO using the CRISP utility so it may not match the version shown here. So if, for example, the ISO was built on a machine configured with a UK locale it will be displayed as .

By default the standard display uses a keyboard layout to match the default locale as discussed above. However, this may be changed to one of the listed alternatives. Note that this does not

Copyright © 1998-2014 Cristie Software Ltd.

change the display language which is always English.

Select **Date, Time and Time Zone** to configure the time zone for the recovery.

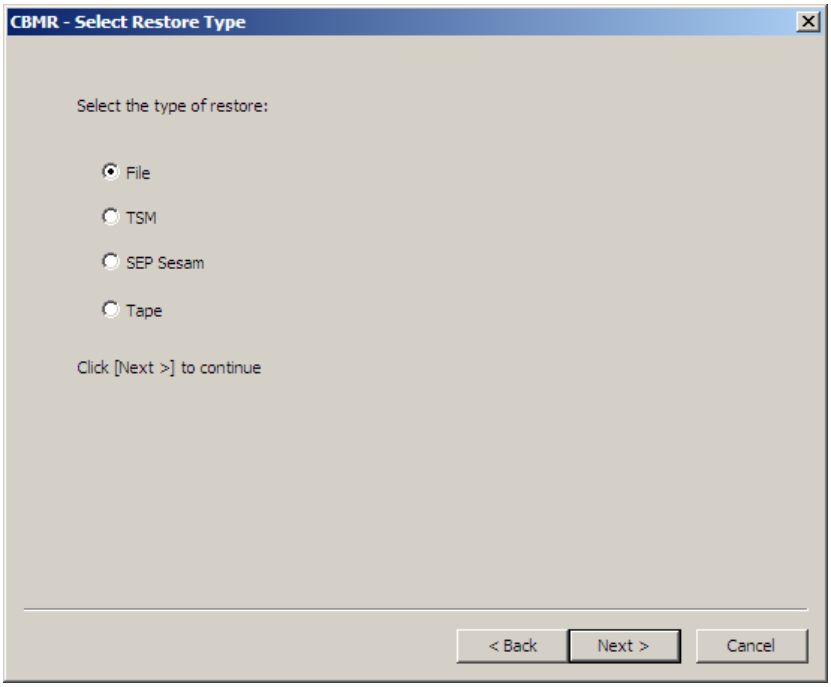

Date and Time
Date and Time
Additional Clocks
Internet Time
Date:
Wednesday, April 16, 2014
Time:
11:27:01 AM
Change date and time...
Time zone
(GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London
Change time zone...
Daylight Saving Time ends on Sunday, October 26, 2014 at 2:00 AM. The clock is set to go back 1 hour at this time.
Remind me one week before this change occurs
How do I set the clock and time zone?
OK
Cancel
Apply

Note: the Additional Clocks and Internet Time tabs are operational. In fact it is possible to synchronise the system time with an NTP time server if required.

Select the Help button to show online help for the recovery environment.

3.4.2.2 Start Automatic Recovery Wizard

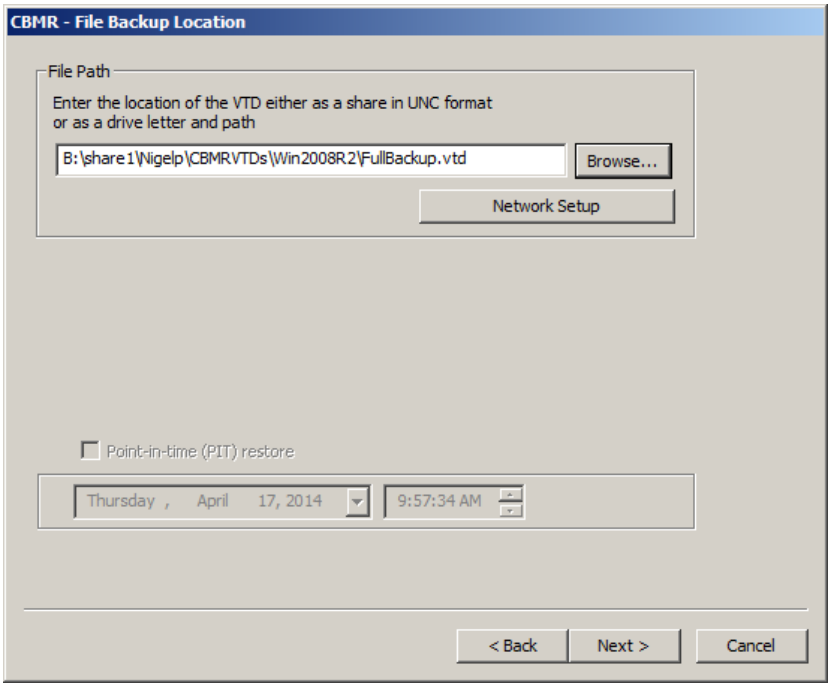
Select this option to commence an **automatic** recovery sequence. The following dialogue prompts you to identify the restore Type.



Press Next> to proceed to the first step of the sequence. Press Cancel to abort the recovery sequence at this point.

File Restore Type

If you selected a **File** restore type, then the following dialogue appears. In the example below the **Network Setup** functionality has been used to map drive **B:** to the location of the backup file in Virtual Tape Drive (VTD) format.



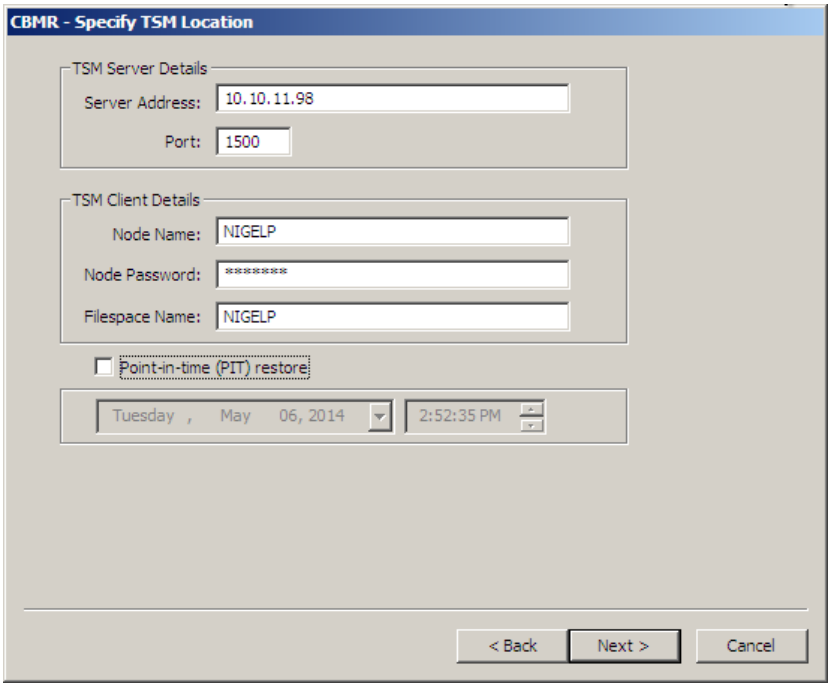
Copyright © 1998-2014 Cristie Software Ltd.

Note Point-in-time (PIT) restore mode is not supported for File type restores.

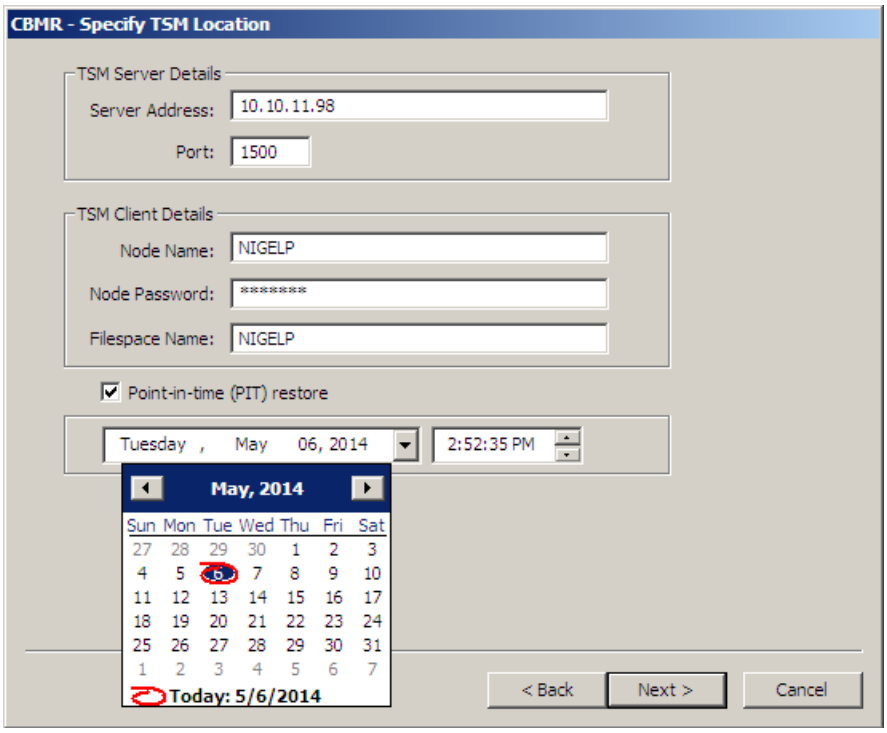
Click Next> to continue.

TSM Restore Type

If you selected a Restore Type of **TSM**, the following dialogue appears. Provide the details for the TSM server and Node used to contain the backup:



Selecting the **Point-in-time** (PIT) restore mode will allow the system to be recovered from the most recent backup before the specified date and time. This means the version of any file restored will be earlier than the specified date and time. Selecting the down-arrow in the calendar control will bring up a calendar:



This can be used to scroll the months/years backwards and forwards as necessary.

Note: a future date will result in the latest backup being recovered.

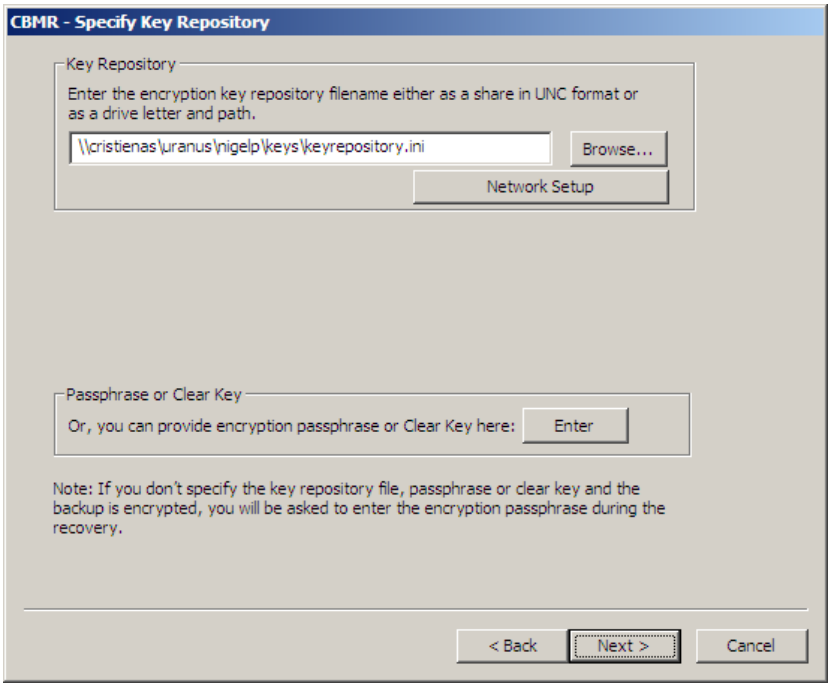
If PIT mode is not selected then, by default, the latest filespace versions will be restored.

Select Next> to continue. At this point the client backup on the specified server will be accessed and the machine configuration extracted.

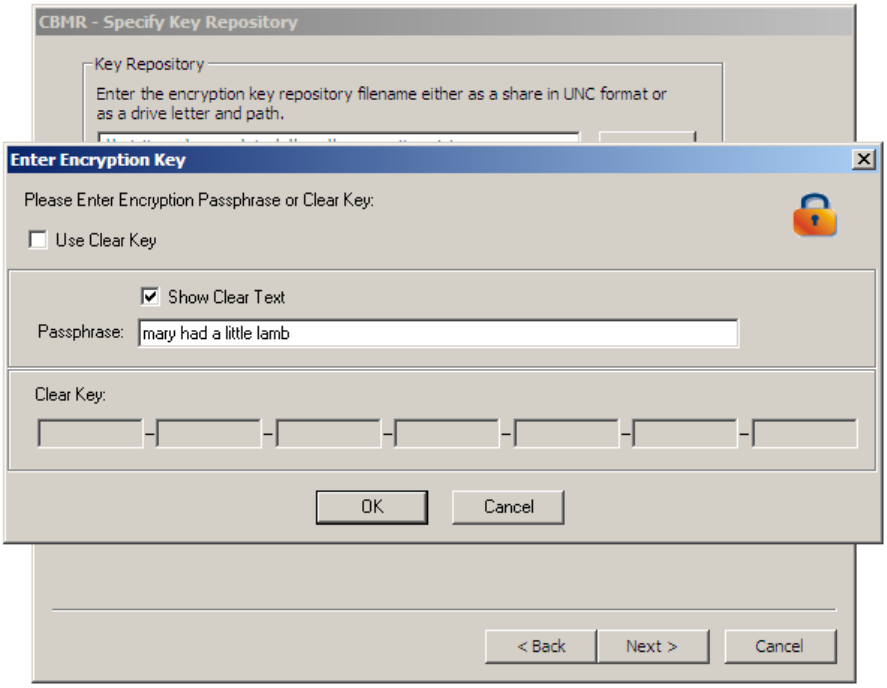
Copyright © 1998-2014 Cristie Software Ltd.

Specify Key Repository

Select Next> to specify a **Key Repository** path, **Passphrase** or **Clear Key**. These parameters are used if the backup is encrypted. If a key or passphrase is not used you may skip this step.


CBMR - Specify Key Repository
Key Repository
Enter the encryption key repository filename either as a share in UNC format or as a drive letter and path.
\\cristienas\uranus\nigelp\keys\keyrepository.ini
Browse...
Network Setup
Passphrase or Clear Key
Or, you can provide encryption passphrase or Clear Key here:
Enter
Note: If you don't specify the key repository file, passphrase or clear key and the backup is encrypted, you will be asked to enter the encryption passphrase during the recovery.
< Back
Next >
Cancel

If the backup was encrypted and no Key Repository file has been entered, then a prompt will appear for the encryption key or passphrase to be manually specified. For example:

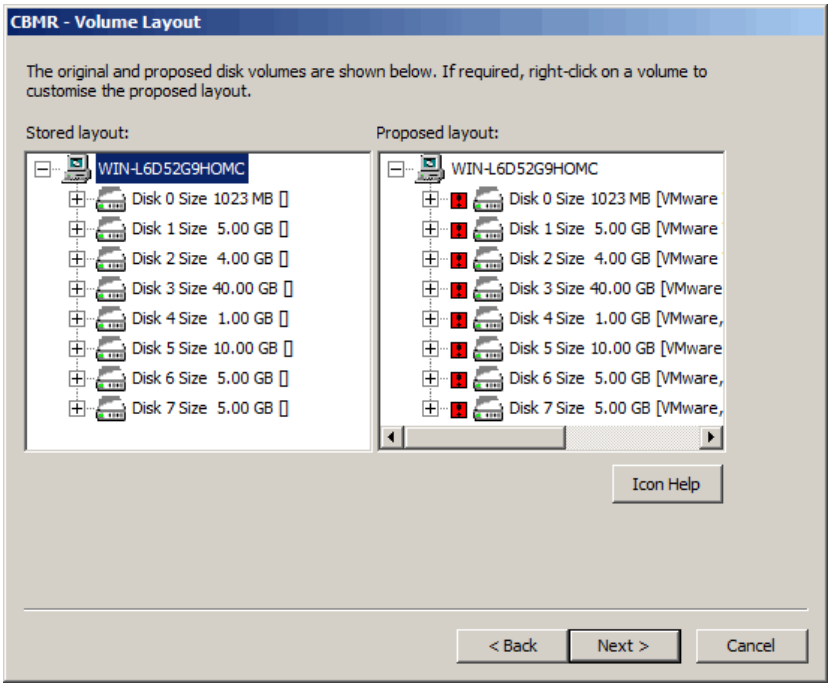

CBMR - Specify Key Repository
Key Repository
Enter the encryption key repository filename either as a share in UNC format or as a drive letter and path.
Enter Encryption Key
Please Enter Encryption Passphrase or Clear Key:
Use Clear Key
Show Clear Text
Passphrase:
mary had a little lamb
Clear Key:
OK
Cancel
< Back
Next >
Cancel

It is not possible to recover the configuration files from an encrypted backup without the key or passphrase.

Select Next> to continue to **Confirm Volume Layout.**

Confirm Volume Layout

The next step in the recovery shows a list of the disks and partitions to be recovered.


CBMR - Volume Layout
The original and proposed disk volumes are shown below. If required, right-click on a volume to customise the proposed layout.
Stored layout:
Proposed layout:
WIN-L6D52G9HOMC
Disk 0 Size 1023 MB []
Disk 1 Size 5.00 GB []
Disk 2 Size 4.00 GB []
Disk 3 Size 40.00 GB []
Disk 4 Size 1.00 GB []
Disk 5 Size 10.00 GB []
Disk 6 Size 5.00 GB []
Disk 7 Size 5.00 GB []
WIN-L6D52G9HOMC
Disk 0 Size 1023 MB [VMware
Disk 1 Size 5.00 GB [VMware
Disk 2 Size 4.00 GB [VMware
Disk 3 Size 40.00 GB [VMware
Disk 4 Size 1.00 GB [VMware,
Disk 5 Size 10.00 GB [VMware
Disk 6 Size 5.00 GB [VMware,
Disk 7 Size 5.00 GB [VMware,
Icon Help
< Back
Next >
Cancel

The left-hand panel of the dialogue shows the original disk layout and partitions. The right-hand panel shows how the recovered disks will be partitioned after the recovery.

A green tick box ✅ next to a disk signifies that the disk and its underlying partitions will be left intact. Placed next to a partition/volume means that the corresponding partition/volume **WILL NOT** be partitioned.

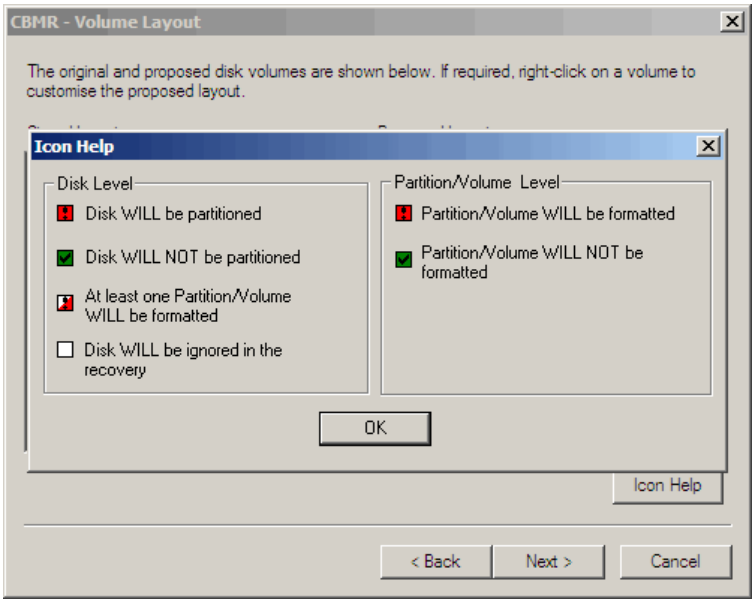
A red exclamation mark ❗ placed next to a disk means it **WILL** be partitioned during recovery. Placed next to a partition or volume means that the corresponding partition/volume **WILL** be partitioned.

A red/white exclamation mark ❗ placed next to a disk means at least one partition/volume **WILL** be partitioned.

A white box ☐ indicates that the disk will be completely ignored during the recovery.

Click on the Icon Help button to display a summary of this:

Copyright © 1998-2014 Cristie Software Ltd.

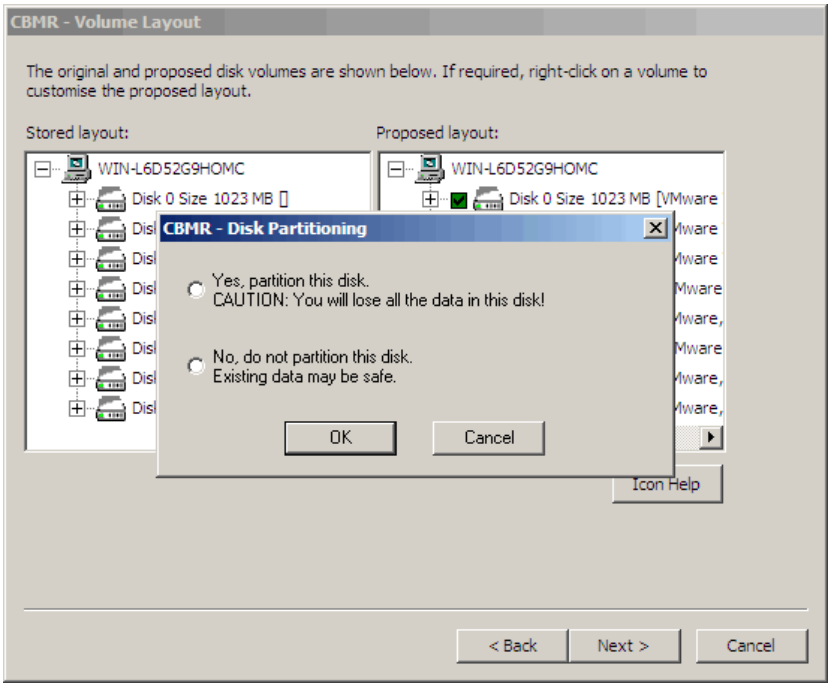

CBMR - Volume Layout
The original and proposed disk volumes are shown below. If required, right-click on a volume to customise the proposed layout.
Icon Help
Disk Level
Disk WILL be partitioned
Disk WILL NOT be partitioned
At least one Partition/Volume WILL be formatted
Disk WILL be ignored in the recovery
Partition/Volume Level
Partition/Volume WILL be formatted
Partition/Volume WILL NOT be formatted
OK
Icon Help
< Back
Next >
Cancel

When the recovery is to the original system, the contents of both panels will look similar if the number of disks is the same. Possibly the disk sizes will be different.

When performing a recovery to a dissimilar system, the disk mapping can be much more complex. Some of the criteria used to judge the disk mapping are:

- disk geometry
- disk capacity
- if currently formatted, the disk signature

You may right-click on any disk shown in the right-hand panel to select whether the disk will be formatted or not.

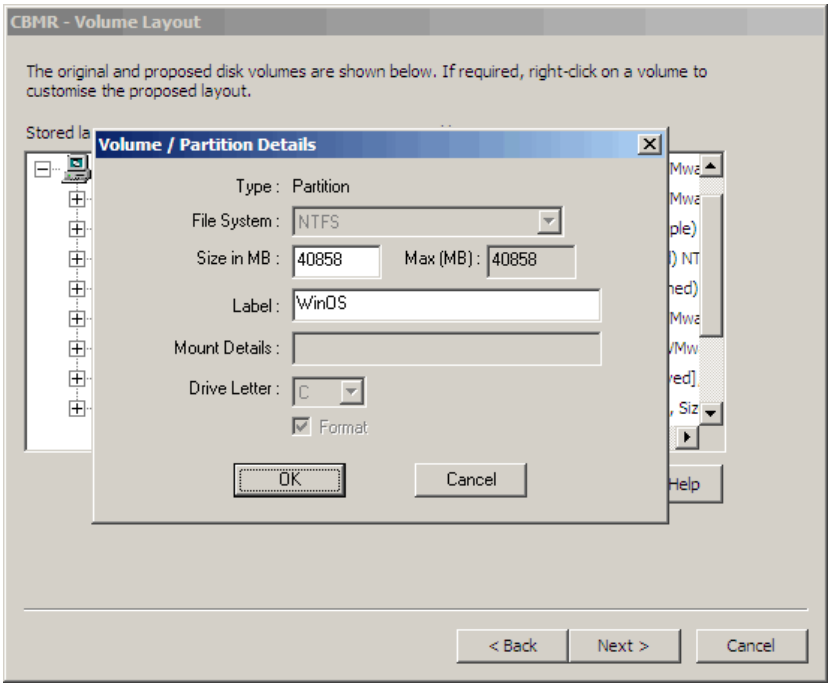

CBMR - Volume Layout
The original and proposed disk volumes are shown below. If required, right-click on a volume to customise the proposed layout.
Stored layout:
Proposed layout:
WIN-L6D52G9HOMC
Disk 0 Size 1023 MB []
WIN-L6D52G9HOMC
Disk 0 Size 1023 MB [VMware
CBMR - Disk Partitioning
Yes, partition this disk.
CAUTION: You will lose all the data in this disk!
No, do not partition this disk.
Existing data may be safe.
OK
Cancel
Icon Help
< Back
Next >
Cancel

Any attempt to incorrectly turn off formatting will result in this error:

CBMR - Disk Partitioning
CBMR - Error
This disk must be repartitioned as the existing disk doesn't match the original disk's layout
OK
OK
Cancel

You may also right-click on a partition to allow you to selectively modify the partition parameters or remove it altogether.

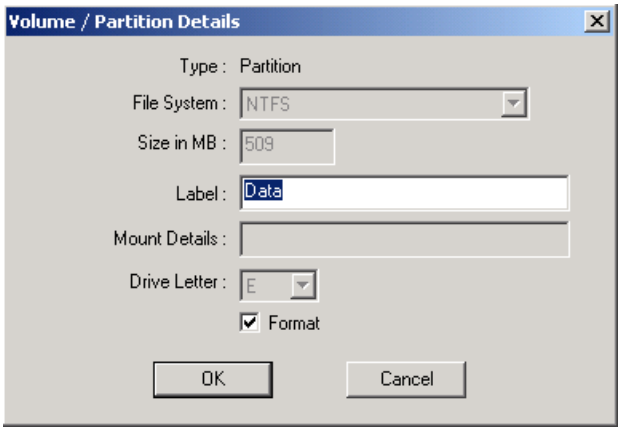
Copyright © 1998-2014 Cristie Software Ltd.



You may **Modify** the following partition parameters:

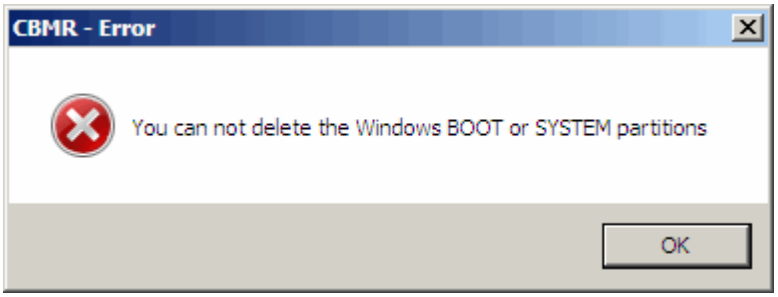
- size in MB (only if disk is shown with a)
- label
- format (yes/no)

The screenshot below shows an example:



Select **Delete** to remove the partition completely (only if disk is shown with a).

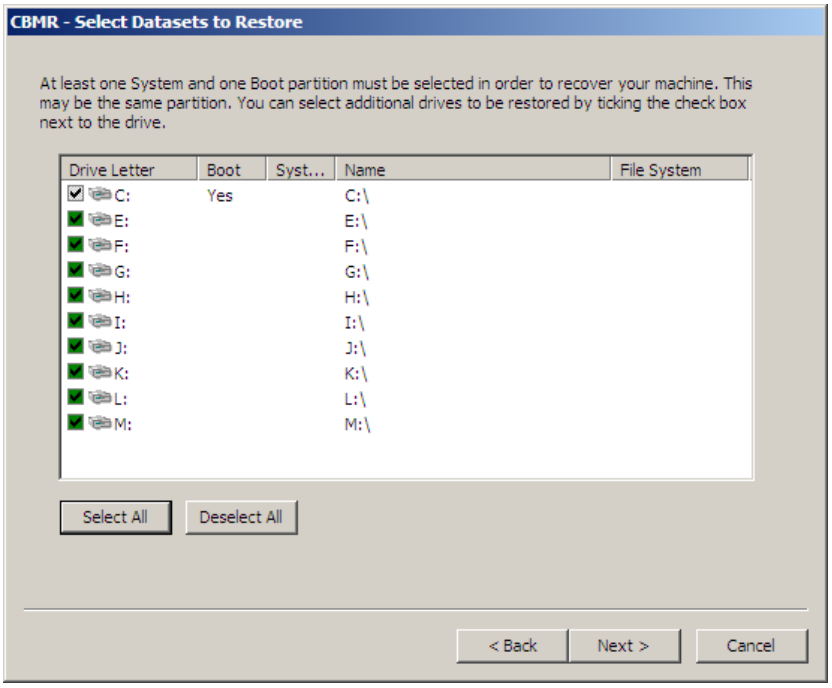
If you attempt to either not format or delete a Windows system partition, an error such as this will be displayed:



At this stage, nothing has happened to the disks. Press Next> to continue with the recovery.

Select Datasets to Restore

The next step prompts for the datasets to restore. Generally, each dataset represents a disk partition or volume. Put a tick against each dataset that should be restored:

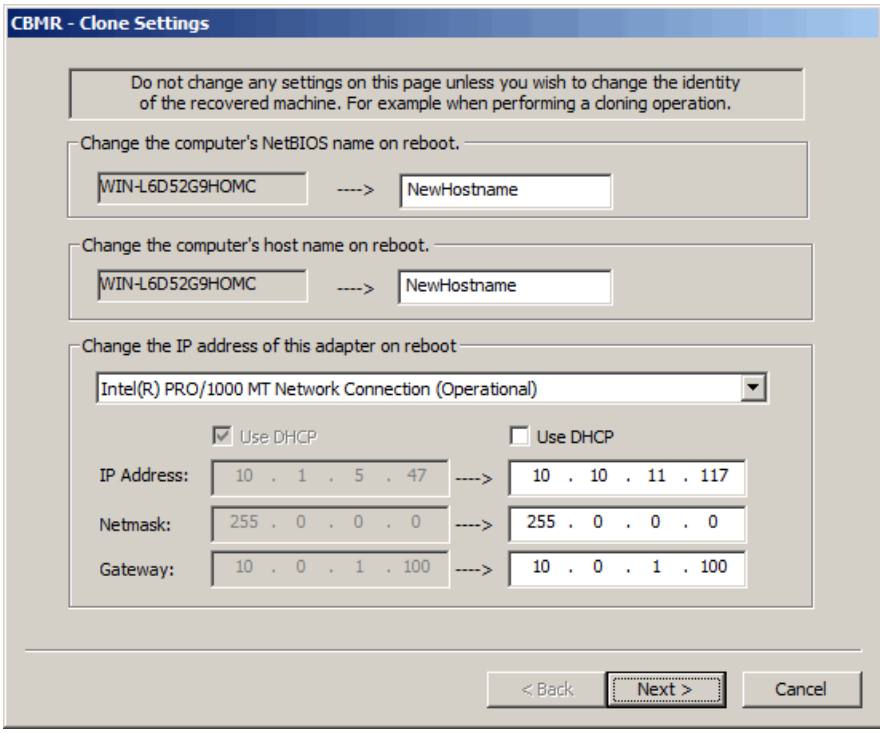

CBMR - Select Datasets to Restore
At least one System and one Boot partition must be selected in order to recover your machine. This may be the same partition. You can select additional drives to be restored by ticking the check box next to the drive.
Drive Letter
Boot
Syst...
Name
File System
C: Yes C:\
E: E:\
F: F:\
G: G:\
H: H:\
I: I:\
J: J:\
K: K:\
L: L:\
M: M:\
Select All
Deselect All
< Back
Next >
Cancel

Click Next> to continue to the **Clone Settings** dialogue.

Copyright © 1998-2014 Cristie Software Ltd.

Clone Settings

Use this dialogue to change the recovered system's **hostname** and **IP addresses** if required. Select to use either DHCP or enter a valid static IP address.

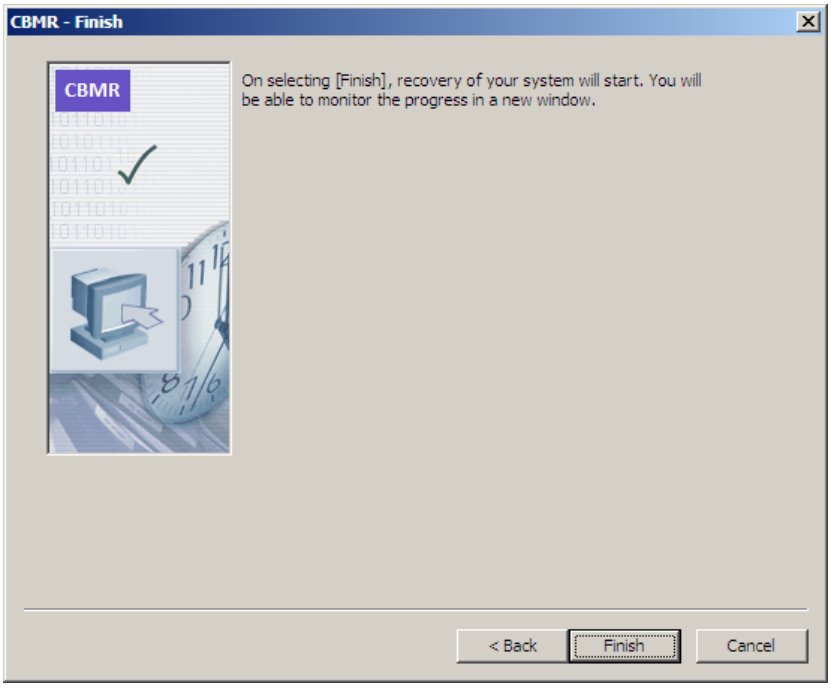

CBMR - Clone Settings
Do not change any settings on this page unless you wish to change the identity of the recovered machine. For example when performing a cloning operation.
Change the computer's NetBIOS name on reboot.
WIN-L6D52G9HOMC
---->
NewHostname
Change the computer's host name on reboot.
WIN-L6D52G9HOMC
---->
NewHostname
Change the IP address of this adapter on reboot
Intel(R) PRO/1000 MT Network Connection (Operational)
Use DHCP
Use DHCP
IP Address:
10 . 1 . 5 . 47
---->
10 . 10 . 11 . 117
Netmask:
255 . 0 . 0 . 0
---->
255 . 0 . 0 . 0
Gateway:
10 . 0 . 1 . 100
---->
10 . 0 . 1 . 100
< Back
Next >
Cancel

You may change the IP address for each NIC interface independently. NICs that are currently connected to a network are tagged with **(Operational)**.

If you wish to retain the current hostname and IP addresses leave the fields at their default values and select Next> to continue to the next section.

Proceed With The Recovery

Before continuing with the actual recovery a final warning screen is displayed.


CBMR - Finish
CBMR
On selecting [Finish], recovery of your system will start. You will be able to monitor the progress in a new window.
< Back
Finish
Cancel

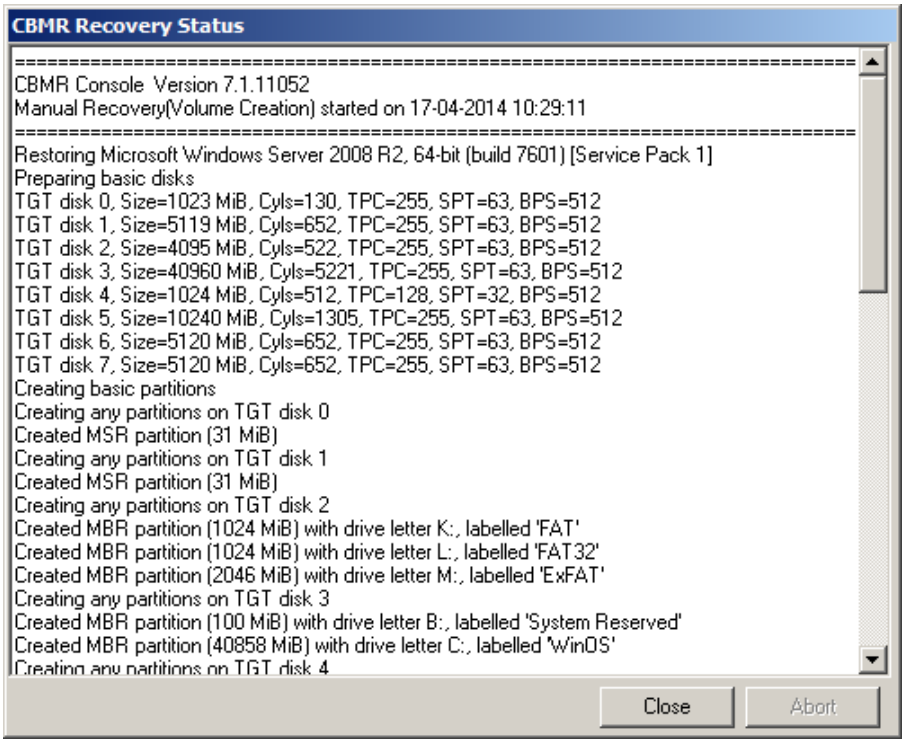
If you are happy with the recovery configuration, press Finish. This will commence the **actual** recovery.

> ***Note: this procedure will COMPLETELY DESTROY any existing data on disks selected for format (ie shown with a). Disks or partitions tagged as no format (ie. shown with a) will be retained.***

Copyright © 1998-2014 Cristie Software Ltd.

Disk Recovery Sequence

The sequence begins by preparing the disks selected for formatting.

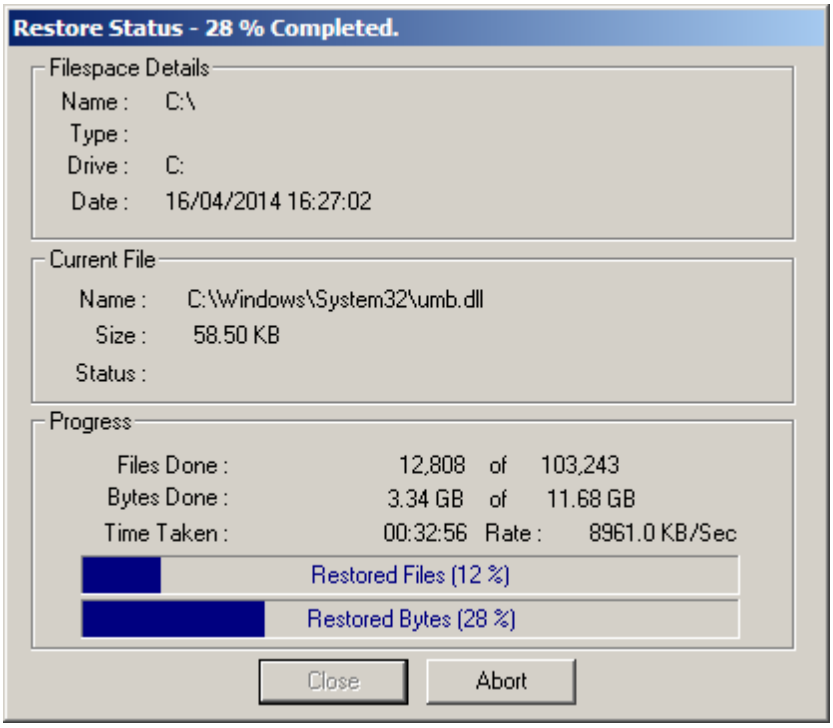

CBMR Recovery Status
CBMR Console Version 7.1.11052
Manual Recovery(Volume Creation) started on 17-04-2014 10:29:11
Restoring Microsoft Windows Server 2008 R2, 64-bit (build 7601) [Service Pack 1]
Preparing basic disks
TGT disk 0, Size=1023 MiB, Cyls=130, TPC=255, SPT=63, BPS=512
TGT disk 1, Size=5119 MiB, Cyls=652, TPC=255, SPT=63, BPS=512
TGT disk 2, Size=4095 MiB, Cyls=522, TPC=255, SPT=63, BPS=512
TGT disk 3, Size=40960 MiB, Cyls=5221, TPC=255, SPT=63, BPS=512
TGT disk 4, Size=1024 MiB, Cyls=512, TPC=128, SPT=32, BPS=512
TGT disk 5, Size=10240 MiB, Cyls=1305, TPC=255, SPT=63, BPS=512
TGT disk 6, Size=5120 MiB, Cyls=652, TPC=255, SPT=63, BPS=512
TGT disk 7, Size=5120 MiB, Cyls=652, TPC=255, SPT=63, BPS=512
Creating basic partitions
Creating any partitions on TGT disk 0
Created MSR partition (31 MiB)
Creating any partitions on TGT disk 1
Created MSR partition (31 MiB)
Creating any partitions on TGT disk 2
Created MBR partition (1024 MiB) with drive letter K:, labelled 'FAT'
Created MBR partition (1024 MiB) with drive letter L:, labelled 'FAT32'
Created MBR partition (2046 MiB) with drive letter M:, labelled 'ExFAT'
Creating any partitions on TGT disk 3
Created MBR partition (100 MiB) with drive letter B:, labelled 'System Reserved'
Created MBR partition (40858 MiB) with drive letter C:, labelled 'WinOS'
Creating any partitions on TGT disk 4
Close
Abort

This step involves:

- disk mapping original layout to new
- cleaning (removing any existing disk partitions)
- removing any existing dynamic volume databases
- re-creating the partitions on selected disks
- converting to dynamic volumes if required
- formatting to the required partition type
- creating partition/volume mount points
- making bootable volumes active

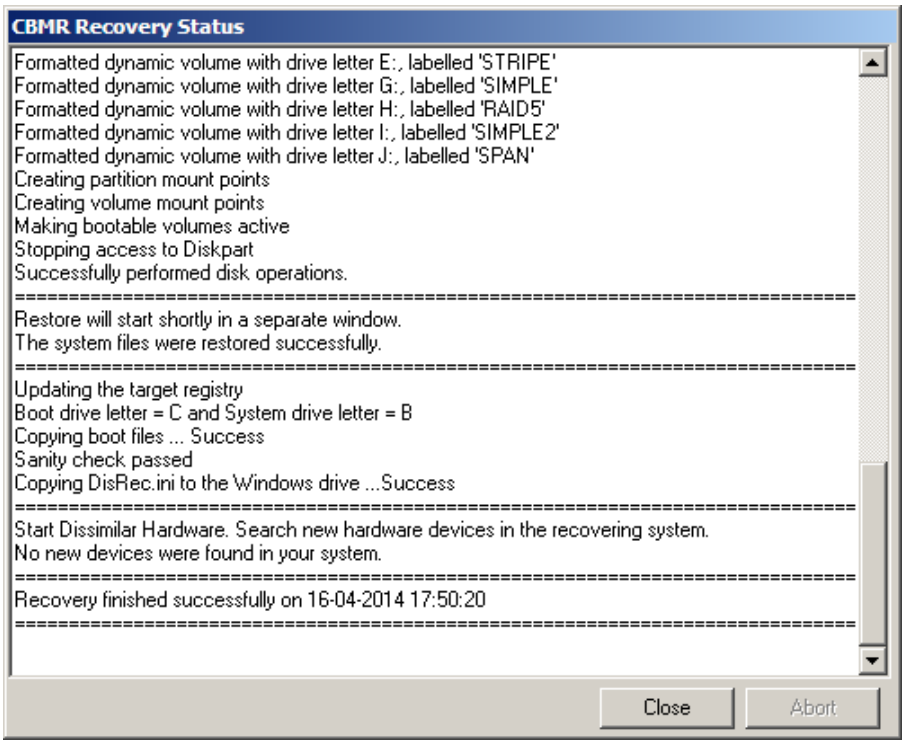
The next step is to recover the datasets to the selected target disks/partitions. A new window appears containing the restore status of recovered files, with progress bars indicating how much of the backup has been restored. This display also shows the recovery statistics in terms of time, size and throughput.

The recovery is divided into different phases: *SystemState*, followed by the recovery of each *volume dataset* selected:



This process may take some minutes if the backups are large. You may select the Abort button to terminate the file recovery process, but this may leave the disk or partition in an unpredictable state, which may render it unusable.

If any errors occur during the recovery, an error message will be shown in the dialogue window. Refer to the logs post recovery to establish the cause of any error.


CBMR Recovery Status
Formatted dynamic volume with drive letter E:, labelled 'STRIPE'
Formatted dynamic volume with drive letter G:, labelled 'SIMPLE'
Formatted dynamic volume with drive letter H:, labelled 'RAID5'
Formatted dynamic volume with drive letter I:, labelled 'SIMPLE2'
Formatted dynamic volume with drive letter J:, labelled 'SPAN'
Creating partition mount points
Creating volume mount points
Making bootable volumes active
Stopping access to Diskpart
Successfully performed disk operations.
Restore will start shortly in a separate window.
The system files were restored successfully.
Updating the target registry
Boot drive letter = C and System drive letter = B
Copying boot files ... Success
Sanity check passed
Copying DisRec.ini to the Windows drive ...Success
Start Dissimilar Hardware. Search new hardware devices in the recovering system.
No new devices were found in your system.
Recovery finished successfully on 16-04-2014 17:50:20
Close
Abort

The final steps of the recovery are to:

- run a sanity check to determine if all the expected boot files are present on the boot volume

Copyright © 1998-2014 Cristie Software Ltd.

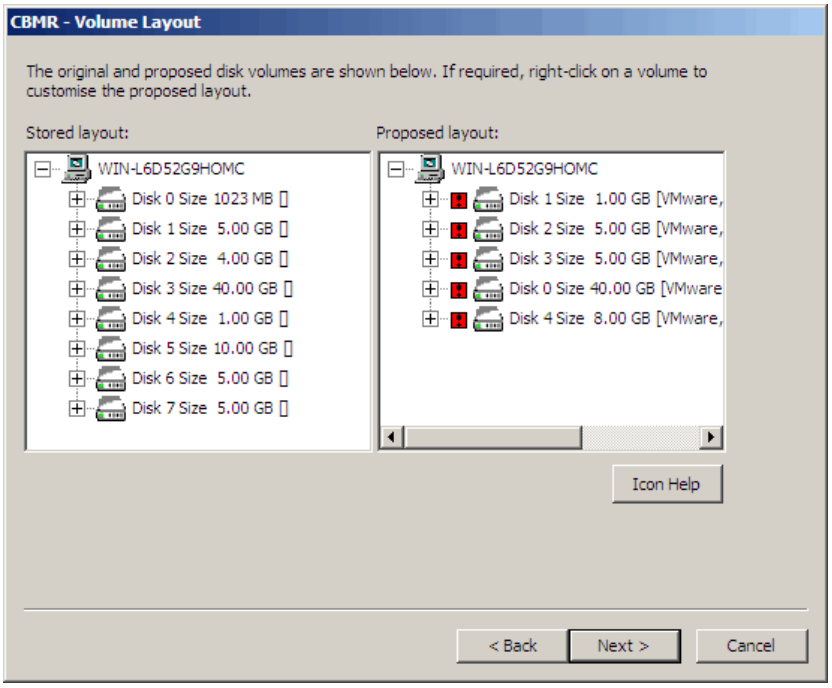
- run a dissimilar hardware check to determine if new drivers are required for new boot devices

Finally, press Close to return to the **Recovery Console** main menu. At this point, you may want to view the recovery logs and perhaps copy the logs to a local device or remote share before selecting to reboot.

> ***Note: Recovery logs are also saved to the recovered system to the CBMR installation sub-folder 'Temp' (e.g. "C:\Program Files\Cristie\CBMR\Temp")***

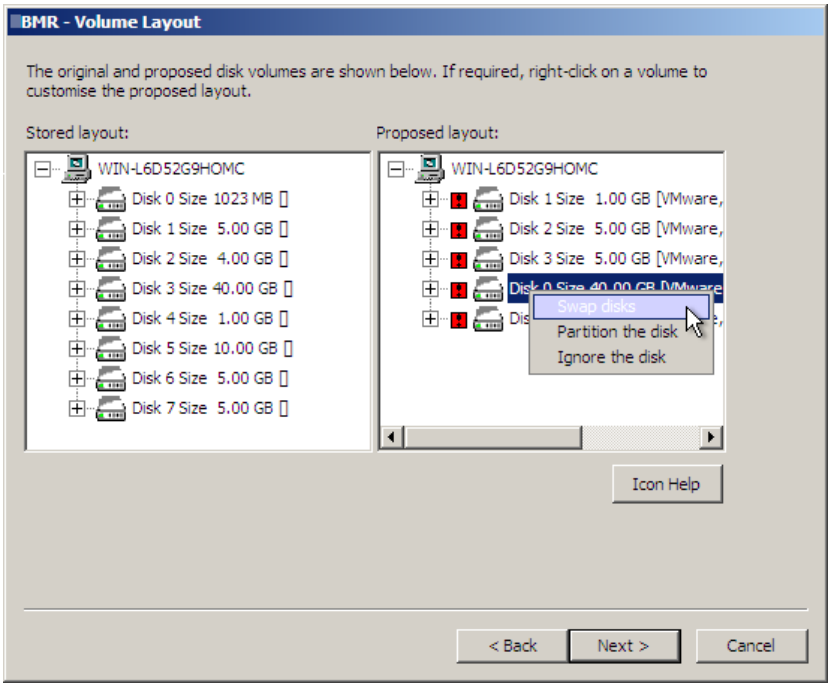
Disk Scaling

In situations where the target system has fewer or smaller disks than the original system, *Disk Scaling* will come into effect.

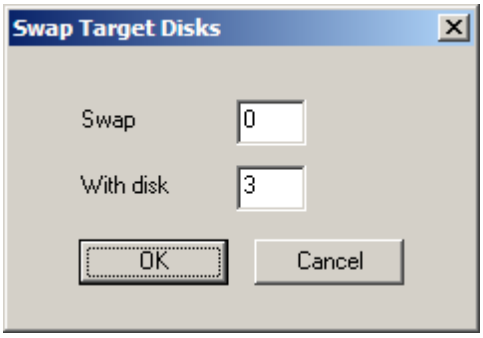

CBMR - Volume Layout
The original and proposed disk volumes are shown below. If required, right-click on a volume to customise the proposed layout.
Stored layout:
WIN-L6D52G9HOMC
Disk 0 Size 1023 MB
Disk 1 Size 5.00 GB
Disk 2 Size 4.00 GB
Disk 3 Size 40.00 GB
Disk 4 Size 1.00 GB
Disk 5 Size 10.00 GB
Disk 6 Size 5.00 GB
Disk 7 Size 5.00 GB
Proposed layout:
WIN-L6D52G9HOMC
Disk 1 Size 1.00 GB [VMware,
Disk 2 Size 5.00 GB [VMware,
Disk 3 Size 5.00 GB [VMware,
Disk 0 Size 40.00 GB [VMware
Disk 4 Size 8.00 GB [VMware,
Icon Help
< Back
Next >
Cancel

The above example shows a recovery from an original system with many physical disks to a target system with fewer disks. One of the target disks is also smaller than the original system disk.

You make need to invoke 'Map disks automatically' from the **Tools/Advanced** menu in this situation to ensure the source/target disks are mapped correctly. Ensure you do this before the recovery sequence is started. If automatic disk mapping does not provide the intended configuration you can also adjust the mapping manually by right-clicking on a disk in the target area and choosing the **Swap disk** feature.


BMR - Volume Layout
The original and proposed disk volumes are shown below. If required, right-click on a volume to customise the proposed layout.
Stored layout:
Proposed layout:
WIN-L6D52G9HOMC
Disk 0 Size 1023 MB
Disk 1 Size 5.00 GB
Disk 2 Size 4.00 GB
Disk 3 Size 40.00 GB
Disk 4 Size 1.00 GB
Disk 5 Size 10.00 GB
Disk 6 Size 5.00 GB
Disk 7 Size 5.00 GB
WIN-L6D52G9HOMC
Disk 1 Size 1.00 GB [VMware,
Disk 2 Size 5.00 GB [VMware,
Disk 3 Size 5.00 GB [VMware,
Swap disks
Partition the disk
Ignore the disk
Icon Help
< Back
Next >
Cancel

This will then display a dialogue allowing you to choose which target disks should be swapped in order.



In this scenario, CBMR will select as many disks to recover as possible (in this case only one disk - the boot disk). In addition, it will scale the partitions down in proportion to their original size and occupancy. This can be complicated by having, say, mirrored dynamic volumes when the mirror will need to be broken - if only one disk exists on the target (or it has been tagged as not to modify).

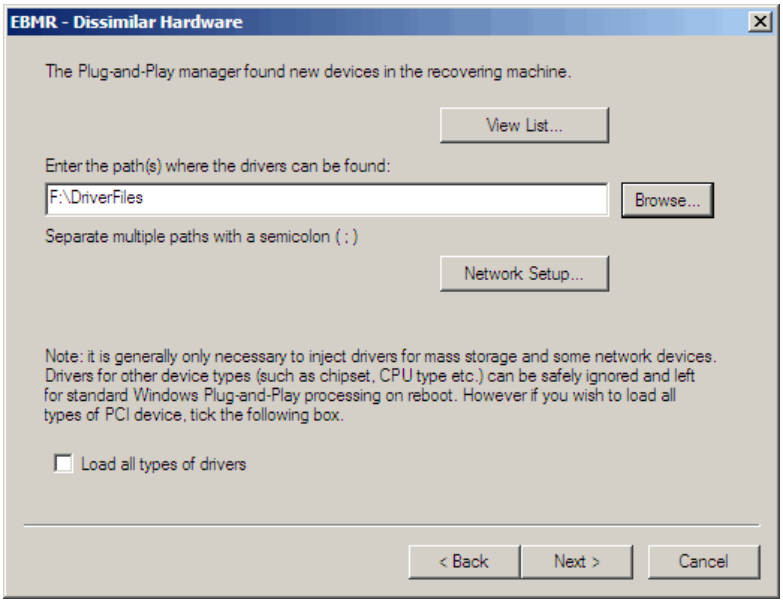
> ***Note: the Volume Layout dialogue will only show disks in the left hand panel that can be removed.***

> ***Note: during a recovery to a system with larger disks, the partition sizes will remain the same as the original by default. However, in this case, it is possible to increase partition size manually during the recovery by right-clicking on the partition icon and selecting Modify.***

Dissimilar Hardware

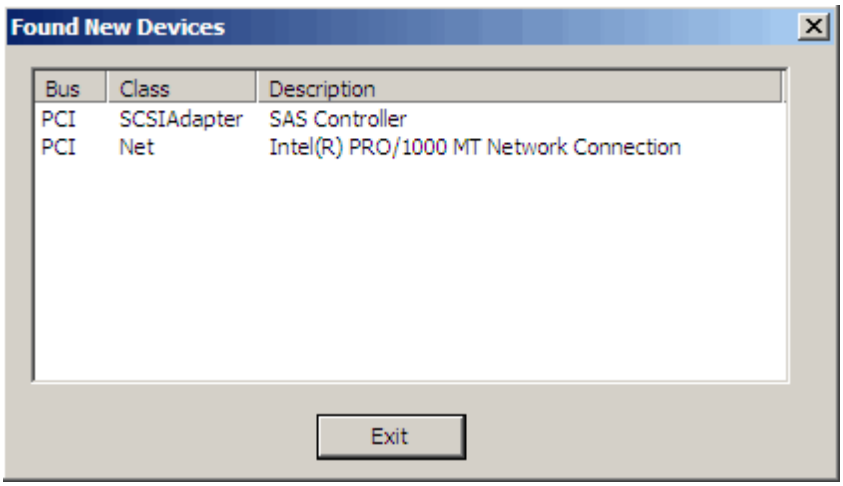
Next, the DR process performs a check to determine if there are new devices in the recovering machine that were not present in the original system. If this is true, then this is a 'dissimilar' DR and the following dialogue will be shown to allow the user to specify the location of the new driver files for these devices.

Copyright © 1998-2014 Cristie Software Ltd.


EBMR - Dissimilar Hardware
The Plug-and-Play manager found new devices in the recovering machine.
View List...
Enter the path(s) where the drivers can be found:
F:\DriverFiles
Browse...
Separate multiple paths with a semicolon (;)
Network Setup...
Note: it is generally only necessary to inject drivers for mass storage and some network devices. Drivers for other device types (such as chipset, CPU type etc.) can be safely ignored and left for standard Windows Plug-and-Play processing on reboot. However if you wish to load all types of PCI device, tick the following box.
Load all types of drivers
< Back
Next >
Cancel

Specify the default path or paths to be searched for the missing driver files. The paths may be on a local device (eg. a USB disk) or a network share. Use the Network Setup... button if you need to map a network share. In either case, the paths must be accessible to the WinPE2 or WinPE4 environment.

Select View List... to see a list of the new devices.



Ensure the specified path or paths contain the correct drivers for the dissimilar machine (ie. correct 32 or 64-bit version as appropriate for the OS). At the end of the DR sequence, the specified paths will be searched for the missing drivers and automatically injected into the recovered system.

By default, it is only necessary to inject drivers for mass storage devices and, in some some cases, network devices. The 'Load all types of drivers' tick box will force the DR to look for all drivers in addition to mass storage and network devices. For example, this could include graphics cards, USB and chipset devices, but these are rarely required and not recommended.

Note that if drivers are not found for the new boot disk then, although WinPE2 or WinPE4 will be able to recover the files to the disk, there is a good chance that it will not boot correctly.

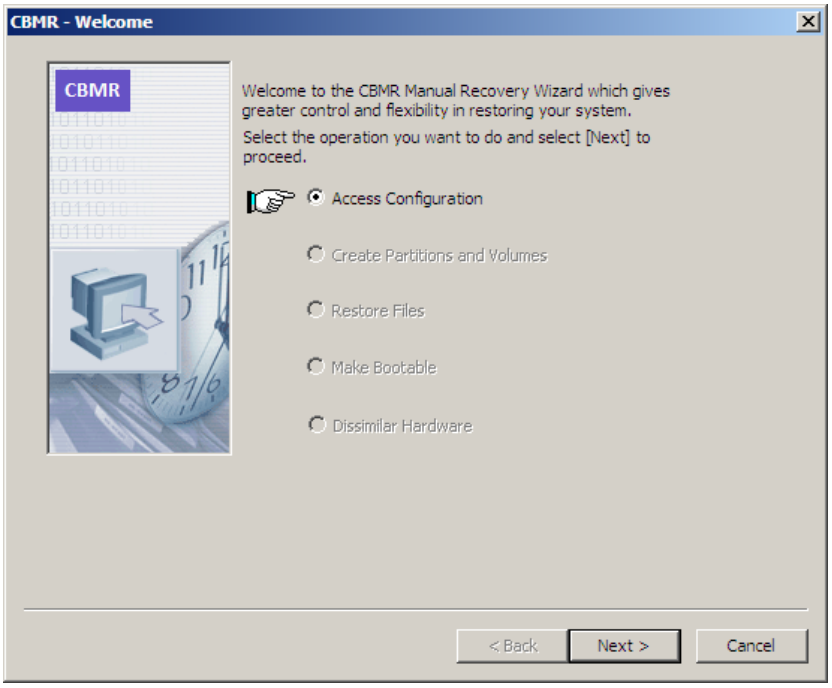
Press Next> to proceed with the recovery.

3.4.2.3 Start Manual Recovery Sequence

Select this option to commence a **manual** recovery sequence.

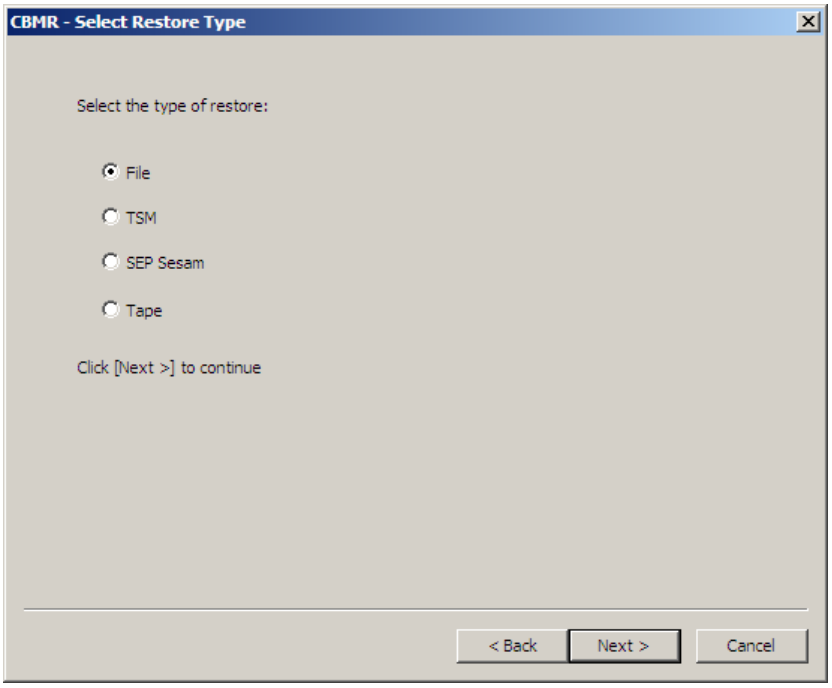
This option will stop after each step in the recovery so allowing the sequence to be aborted or the step to be repeated with different parameters.

The first step of the manual sequence is to provide the location of the DR configuration.


CBMR - Welcome
CBMR
Welcome to the CBMR Manual Recovery Wizard which gives greater control and flexibility in restoring your system.
Select the operation you want to do and select [Next] to proceed.
Access Configuration
Create Partitions and Volumes
Restore Files
Make Bootable
Dissimilar Hardware
< Back
Next >
Cancel

Press Next> to proceed to the first step of the sequence. Press Cancel to abort the recovery sequence at this point.

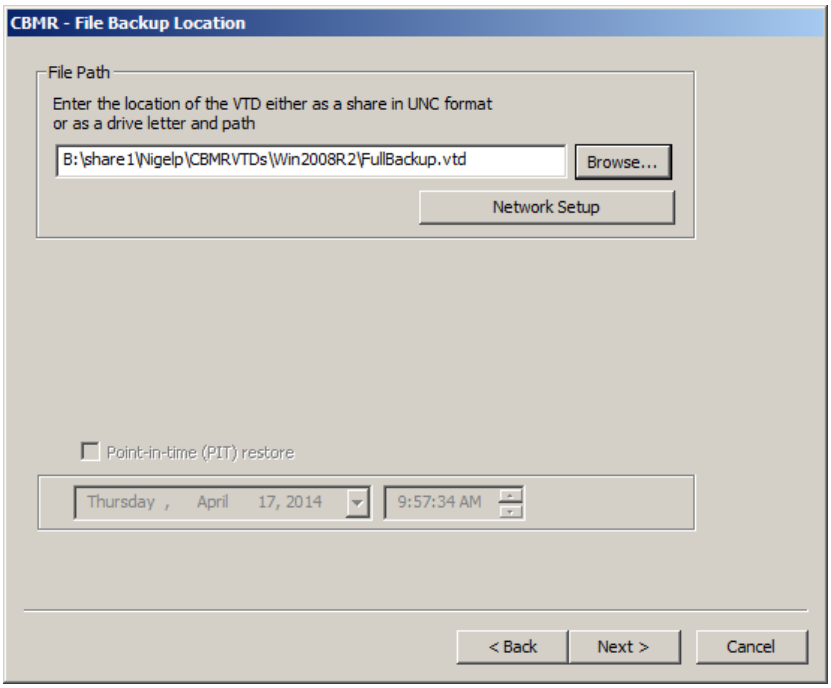
The following dialogue prompts you to identify the restore Type.



Copyright © 1998-2014 Cristie Software Ltd.

File Restore Type

If you selected a restore Type of File, the following dialogue appears. In the example below the Network Setup functionality has been used to map drive B: to the location of the backup file in Virtual Tape Drive (VTD) format.

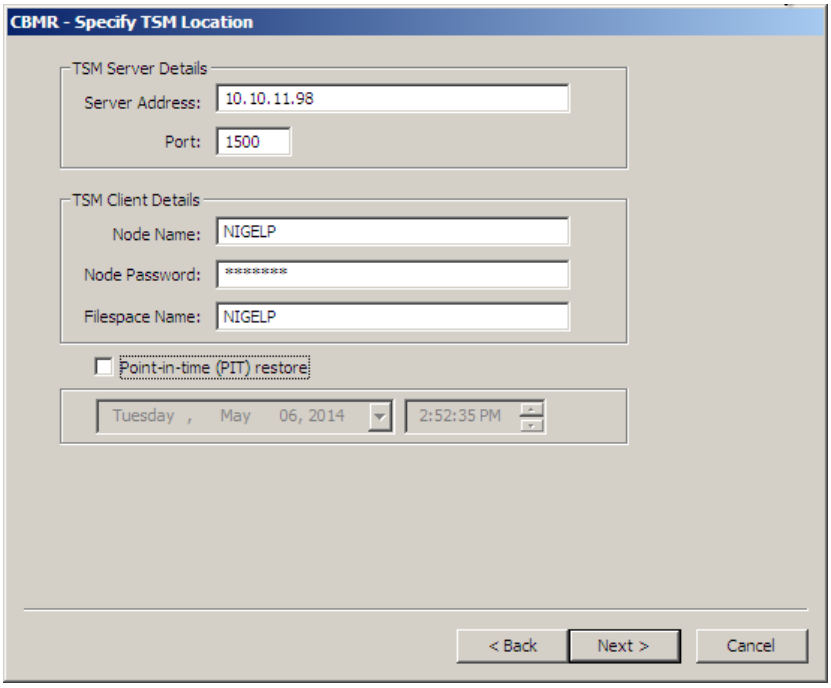


Note Point-in-time (PIT) restore mode is not supported for File type restores.

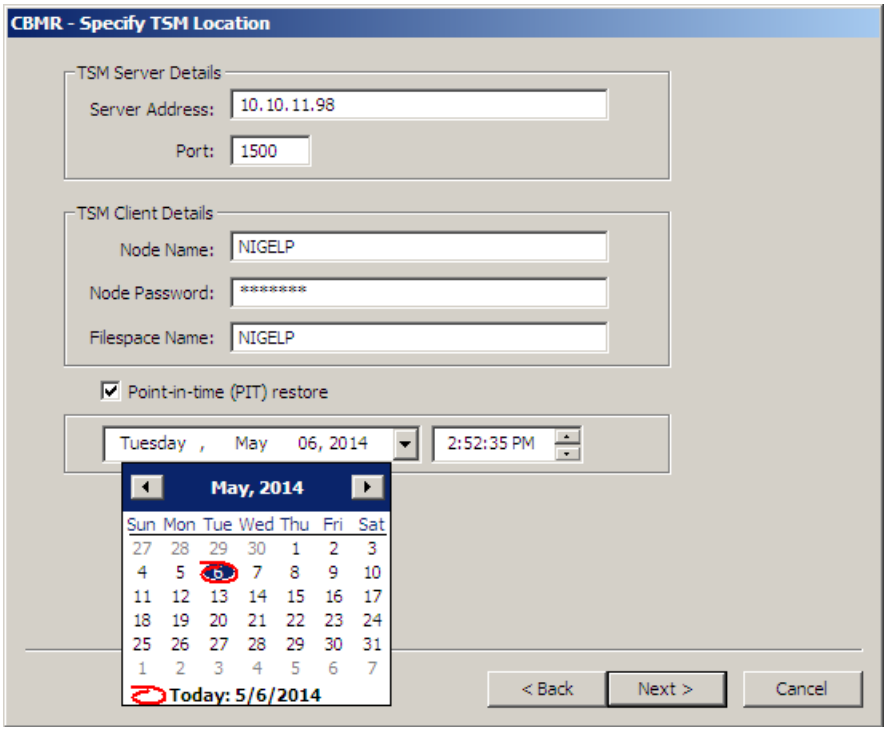
Click Next> to continue.

TSM Restore Type

If you selected a restore type of TSM, the following dialogue appears. Provide the details for the TSM server used for the backup:



Selecting the **Point-in-time** (PIT) restore mode will allow the system to be recovered from the most recent backup before the specified date and time. This means the version of any file restored will be earlier than the specified date and time. Selecting the down-arrow in the calendar control will bring up a calendar:


CBMR - Specify TSM Location
TSM Server Details
Server Address: 10.10.11.98
Port: 1500
TSM Client Details
Node Name: NIGELP
Node Password: ********
Filespace Name: NIGELP
Point-in-time (PIT) restore
Tuesday , May 06, 2014
2:52:35 PM
May, 2014
Sun Mon Tue Wed Thu Fri Sat
27 28 29 30 1 2 3
4 5 6 7 8 9 10
11 12 13 14 15 16 17
18 19 20 21 22 23 24
25 26 27 28 29 30 31
1 2 3 4 5 6 7
Today: 5/6/2014
< Back
Next >
Cancel

This can be used to scroll the months/years backwards and forwards as necessary.

Note: a future date will result in the latest backup being recovered.

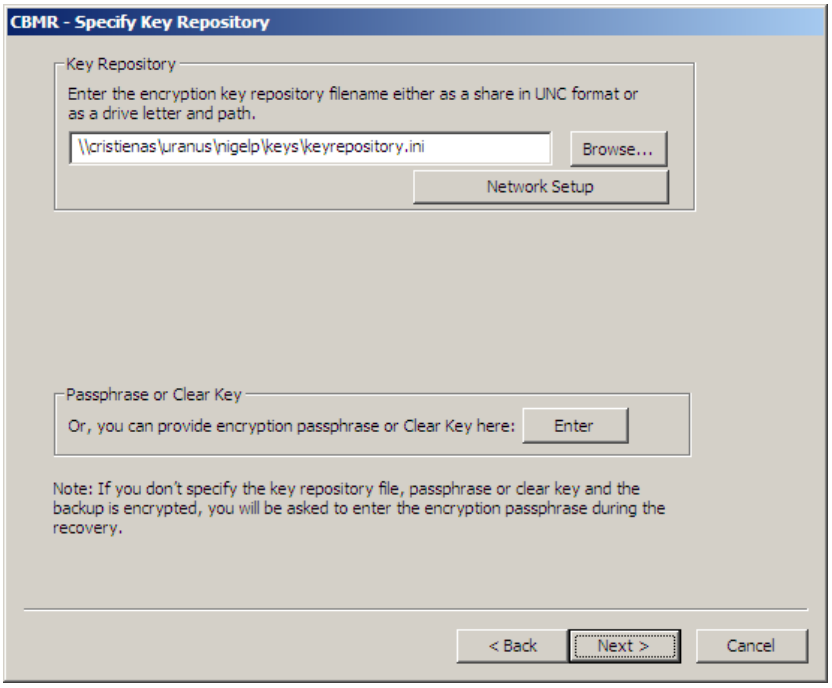
Copyright © 1998-2014 Cristie Software Ltd.

If PIT mode is not selected then, by default, the latest filespace versions will be restored.

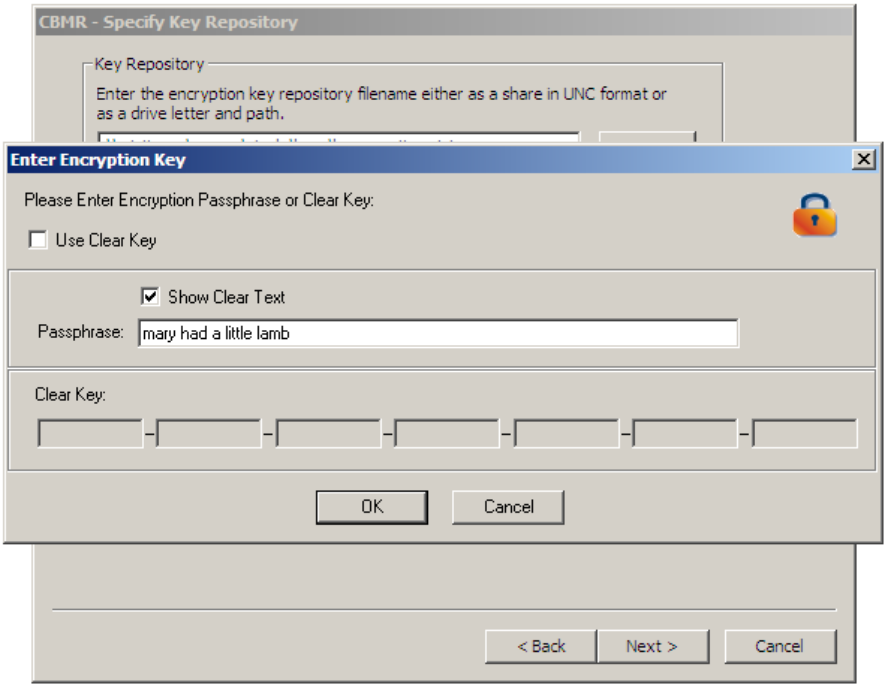
Select Next> to continue. At this point the client backup on the specified server will be accessed and the machine configuration extracted.

Specify Key Repository

Select Next> to specify a **Key Repository** path, **Passphrase** or **Clear Key**. These parameters are used if the backup is encrypted. If a key or passphrase is not used you may skip this step.

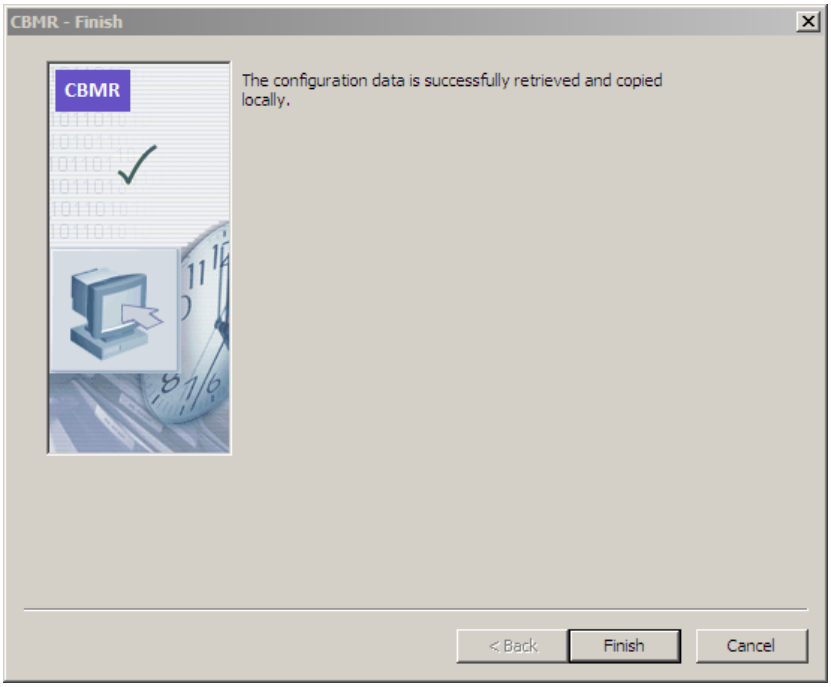

CBMR - Specify Key Repository
Key Repository
Enter the encryption key repository filename either as a share in UNC format or as a drive letter and path.
\\cristienas\uranus\nigelp\keys\keyrepository.ini
Browse...
Network Setup
Passphrase or Clear Key
Or, you can provide encryption passphrase or Clear Key here:
Enter
Note: If you don't specify the key repository file, passphrase or clear key and the backup is encrypted, you will be asked to enter the encryption passphrase during the recovery.
< Back
Next >
Cancel

If the backup was encrypted and no Key Repository file has been entered, then a prompt will appear for the encryption key or passphrase to be manually specified. For example:


CBMR - Specify Key Repository
Key Repository
Enter the encryption key repository filename either as a share in UNC format or as a drive letter and path.
Enter Encryption Key
Please Enter Encryption Passphrase or Clear Key:
Use Clear Key
Show Clear Text
Passphrase:
mary had a little lamb
Clear Key:
OK
Cancel
< Back
Next >
Cancel

It is not possible to recover the configuration files from an encrypted backup without the key or passphrase.

Select Next> and the following dialogue is displayed, indicating that this part of the configuration is complete.

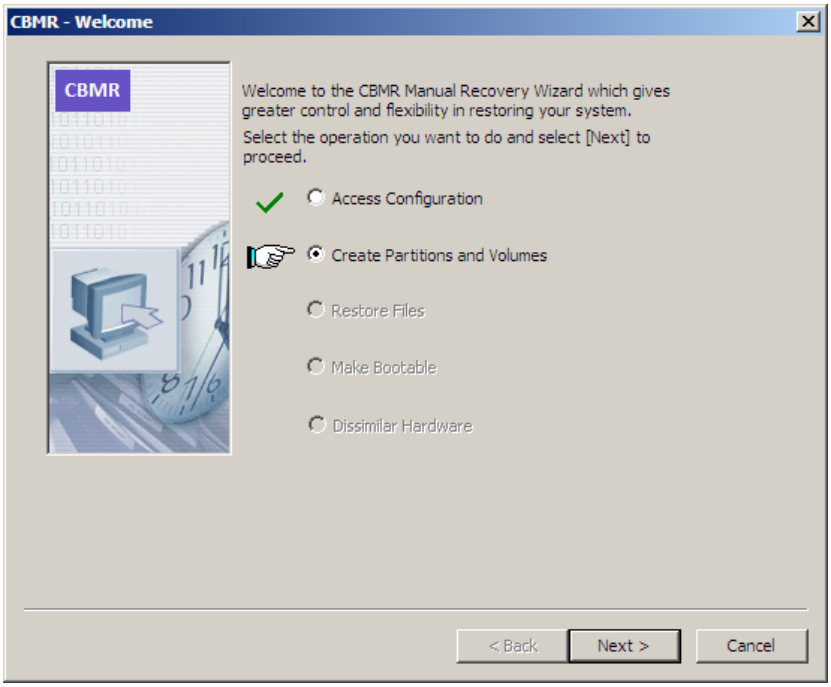


Select Finish to complete the step and return to the **Manual Recovery Wizard**

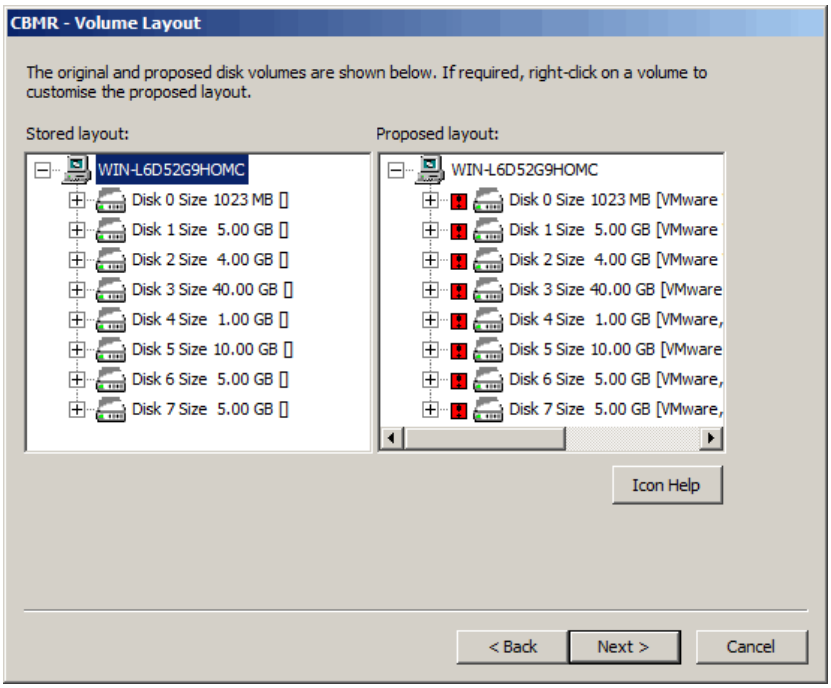
Copyright © 1998-2014 Cristie Software Ltd.

Create Partition and Volumes

The next step of the **Manual Recovery** process is to configure the target disk partitions and volumes.


CBMR - Welcome
CBMR
Welcome to the CBMR Manual Recovery Wizard which gives greater control and flexibility in restoring your system.
Select the operation you want to do and select [Next] to proceed.
Access Configuration
Create Partitions and Volumes
Restore Files
Make Bootable
Dissimilar Hardware
< Back
Next >
Cancel

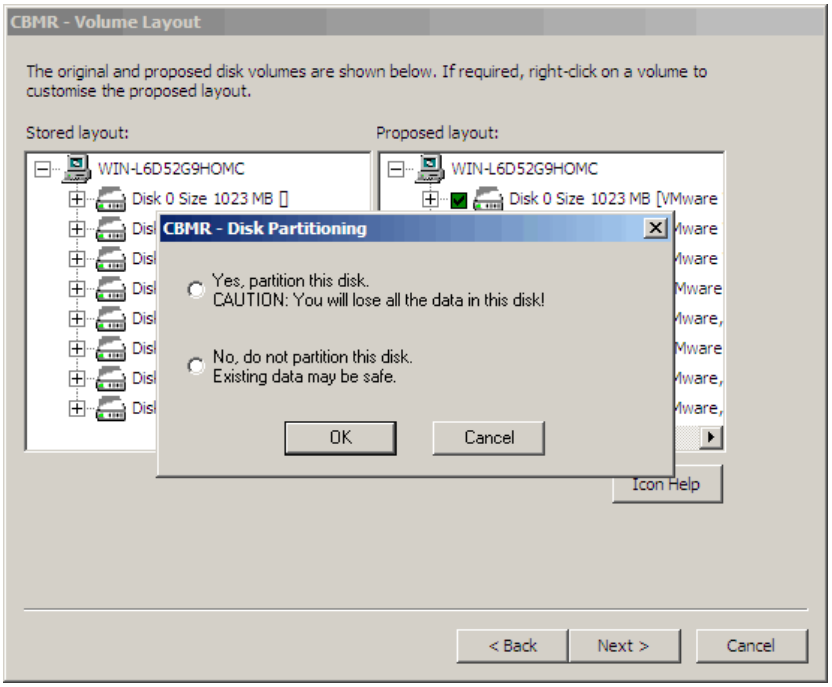
Select Next> to display the Volume Layout dialogue:


CBMR - Volume Layout
The original and proposed disk volumes are shown below. If required, right-click on a volume to customise the proposed layout.
Stored layout:
Proposed layout:
WIN-L6D52G9HOMC
Disk 0 Size 1023 MB []
Disk 1 Size 5.00 GB []
Disk 2 Size 4.00 GB []
Disk 3 Size 40.00 GB []
Disk 4 Size 1.00 GB []
Disk 5 Size 10.00 GB []
Disk 6 Size 5.00 GB []
Disk 7 Size 5.00 GB []
WIN-L6D52G9HOMC
Disk 0 Size 1023 MB [VMware
Disk 1 Size 5.00 GB [VMware
Disk 2 Size 4.00 GB [VMware
Disk 3 Size 40.00 GB [VMware
Disk 4 Size 1.00 GB [VMware,
Disk 5 Size 10.00 GB [VMware
Disk 6 Size 5.00 GB [VMware,
Disk 7 Size 5.00 GB [VMware,
Icon Help
< Back
Next >
Cancel

This screen shows the original disk layout against that of the target system. The target disk layout could be very different to the original. CBMR will attempt to match the disks using its own in-built criteria. Some of the criteria used to judge the match are:

- disk geometry (tracks, cylinders and sectors)
- disk capacity
- if currently formatted, the disk signature

However, it is possible to change the partition size, or opt to tag/untag whether or not a partition should be formatted. To do this, right click on the the disk icon and the following configuration dialogue is displayed:


CBMR - Volume Layout
The original and proposed disk volumes are shown below. If required, right-click on a volume to customise the proposed layout.
Stored layout:
Proposed layout:
WIN-L6D52G9HOMC
Disk 0 Size 1023 MB []
WIN-L6D52G9HOMC
Disk 0 Size 1023 MB [VMware
CBMR - Disk Partitioning
Yes, partition this disk.
CAUTION: You will lose all the data in this disk!
No, do not partition this disk.
Existing data may be safe.
OK
Cancel
Icon Help
< Back
Next >
Cancel

A green tick box ☑ next to a disk signifies that the disk and its underlying partitions will be left intact. Placed next to a partition/volume means that the corresponding partition/volume **WILL NOT** be partitioned.

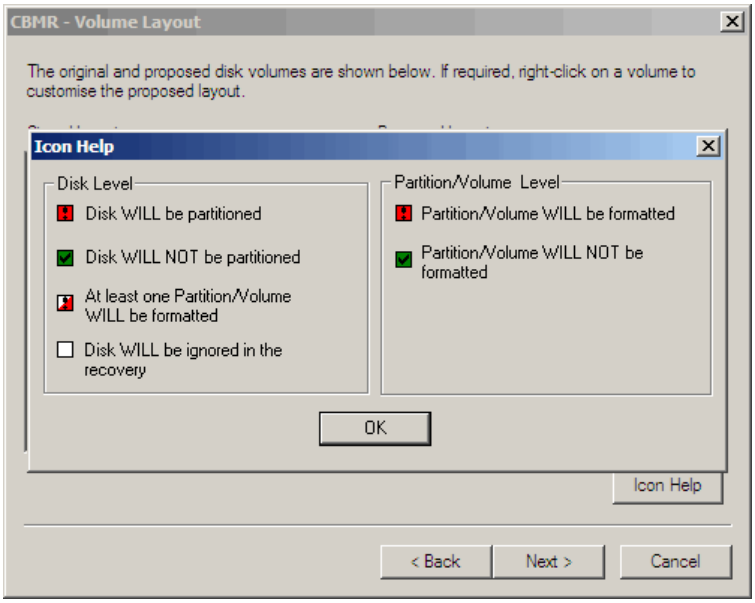
A red exclamation mark ❗ placed next to a disk means it **WILL** be partitioned during recovery. Placed next to a partition or volume means that the corresponding partition/volume **WILL** be partitioned.

A red/white exclamation mark ❗ placed next to a disk means at least one partition/volume **WILL** be partitioned.

A white box ☐ indicates that the disk will be completely ignored during the recovery.

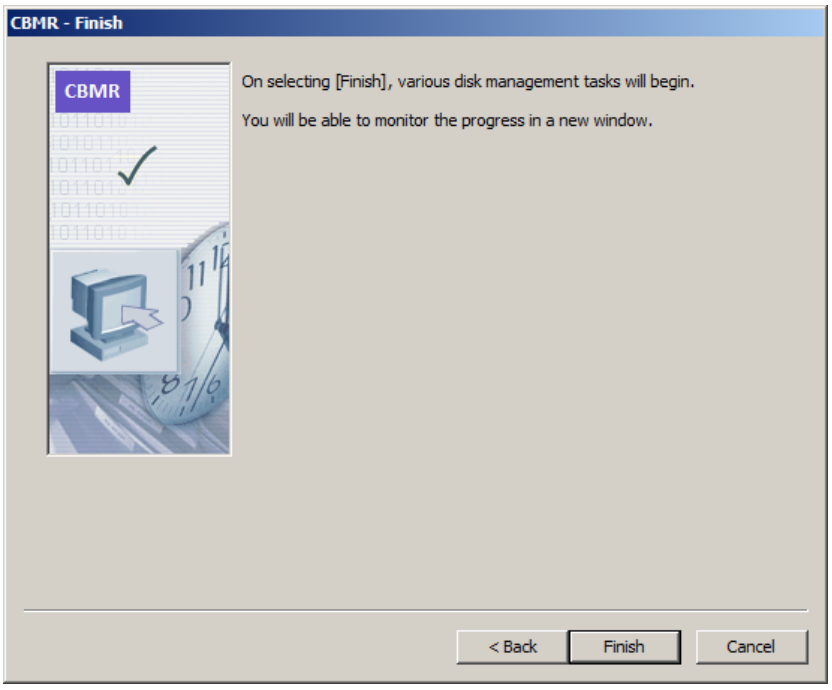
Click on the Icon Help button to display a summary of this:

Copyright © 1998-2014 Cristie Software Ltd.


CBMR - Volume Layout
The original and proposed disk volumes are shown below. If required, right-click on a volume to customise the proposed layout.
Icon Help
Disk Level
Disk WILL be partitioned
Disk WILL NOT be partitioned
At least one Partition/Volume WILL be formatted
Disk WILL be ignored in the recovery
Partition/Volume Level
Partition/Volume WILL be formatted
Partition/Volume WILL NOT be formatted
OK
Icon Help
< Back
Next >
Cancel

Press <Back to return to the previous step, Next> to commence the active part of this step, or Cancel to abort.

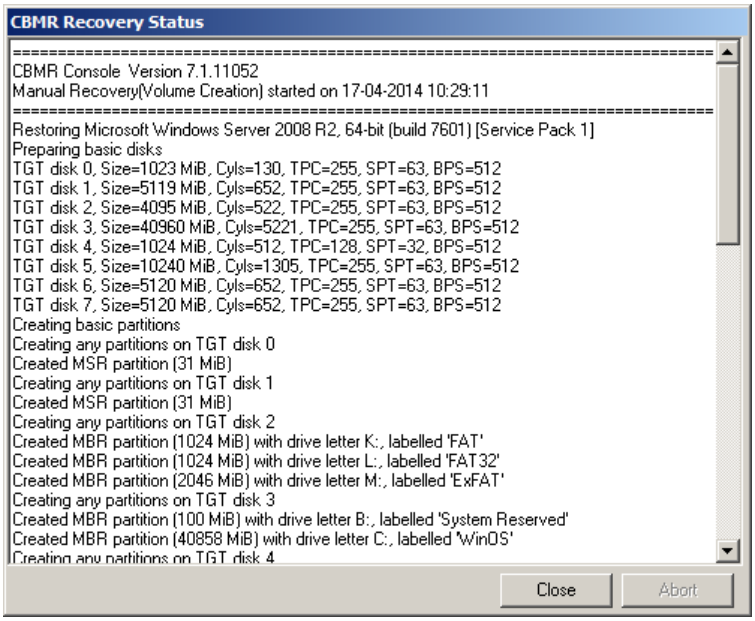
Before continuing with the actual recovery, a final warning dialogue is displayed.


CBMR - Finish
CBMR
On selecting [Finish], various disk management tasks will begin.
You will be able to monitor the progress in a new window.
< Back
Finish
Cancel

If you are happy with the recovery configuration, press Finish. This will begin the physical disk configuration.

> ***Note: this procedure will COMPLETELY DESTROY any existing data on the disks selected for recovery. Disks or partitions tagged as 'no format' will be retained.***

The **Create Partitions and Volumes** step begins by preparing the disk selected for the recovery.


CBMR Recovery Status
CBMR Console Version 7.1.11052
Manual Recovery(Volume Creation) started on 17-04-2014 10:29:11
Restoring Microsoft Windows Server 2008 R2, 64-bit (build 7601) [Service Pack 1]
Preparing basic disks
TGT disk 0, Size=1023 MiB, Cyls=130, TPC=255, SPT=63, BPS=512
TGT disk 1, Size=5119 MiB, Cyls=652, TPC=255, SPT=63, BPS=512
TGT disk 2, Size=4095 MiB, Cyls=522, TPC=255, SPT=63, BPS=512
TGT disk 3, Size=40960 MiB, Cyls=5221, TPC=255, SPT=63, BPS=512
TGT disk 4, Size=1024 MiB, Cyls=512, TPC=128, SPT=32, BPS=512
TGT disk 5, Size=10240 MiB, Cyls=1305, TPC=255, SPT=63, BPS=512
TGT disk 6, Size=5120 MiB, Cyls=652, TPC=255, SPT=63, BPS=512
TGT disk 7, Size=5120 MiB, Cyls=652, TPC=255, SPT=63, BPS=512
Creating basic partitions
Creating any partitions on TGT disk 0
Created MSR partition (31 MiB)
Creating any partitions on TGT disk 1
Created MSR partition (31 MiB)
Creating any partitions on TGT disk 2
Created MBR partition (1024 MiB) with drive letter K:, labelled 'FAT'
Created MBR partition (1024 MiB) with drive letter L:, labelled 'FAT32'
Created MBR partition (2046 MiB) with drive letter M:, labelled 'ExFAT'
Creating any partitions on TGT disk 3
Created MBR partition (100 MiB) with drive letter B:, labelled 'System Reserved'
Created MBR partition (40858 MiB) with drive letter C:, labelled 'WinOS'
Creating any partitions on TGT disk 4
Close
Abort

This involves:

- disk mapping original layout to new
- cleaning (removing any existing disk partitions)
- removing any existing dynamic volume databases
- re-creating the partitions
- converting to dynamic volumes if required
- formatting to the required partition type
- create partition/volume mount points
- make bootable volumes active

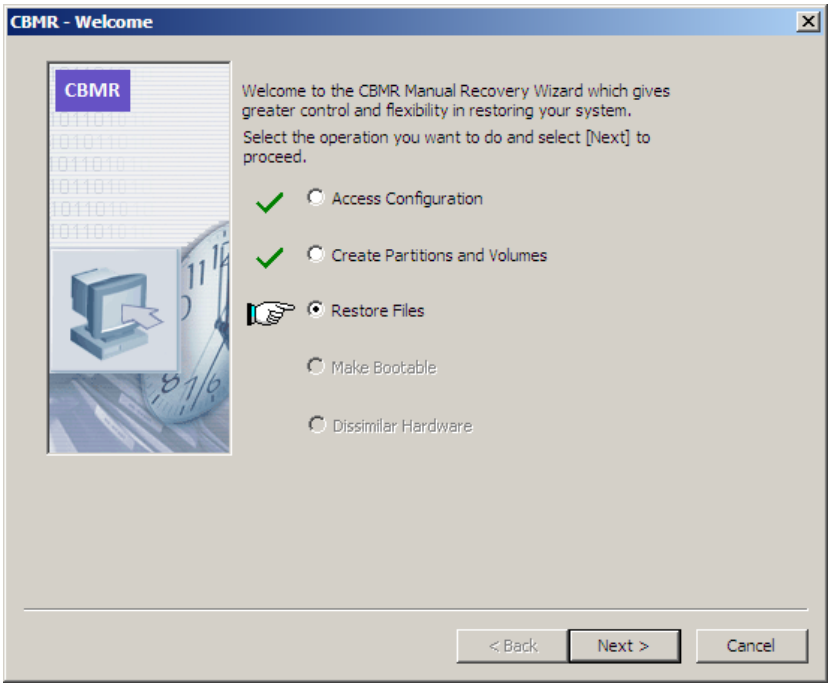
The next step is to recover the backups to the target disks/partitions.

Select Close to complete the step and return to the **Manual Recovery Wizard.**

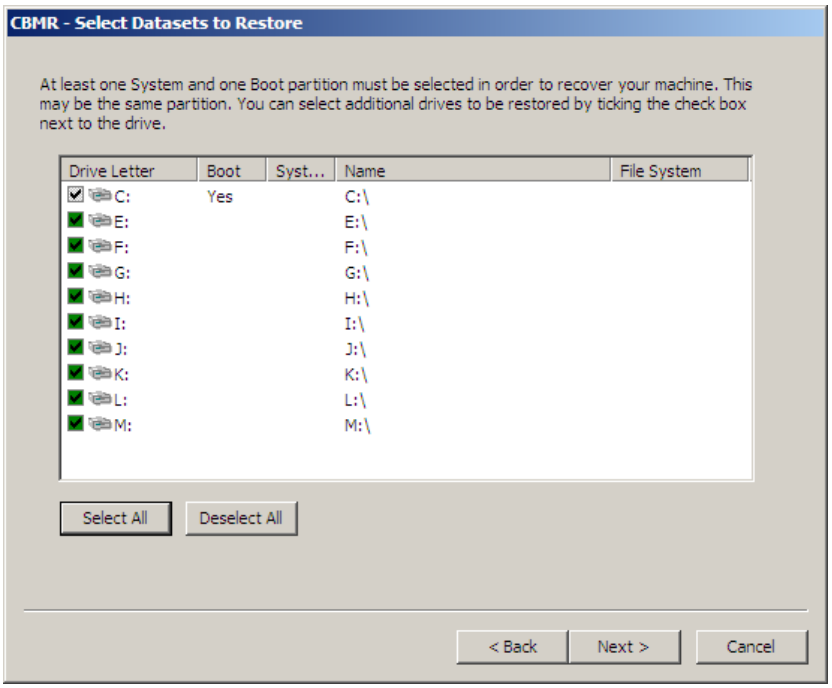
Copyright © 1998-2014 Cristie Software Ltd.

Restore Files

The next step of the manual recovery process is to restore the DR backup files.

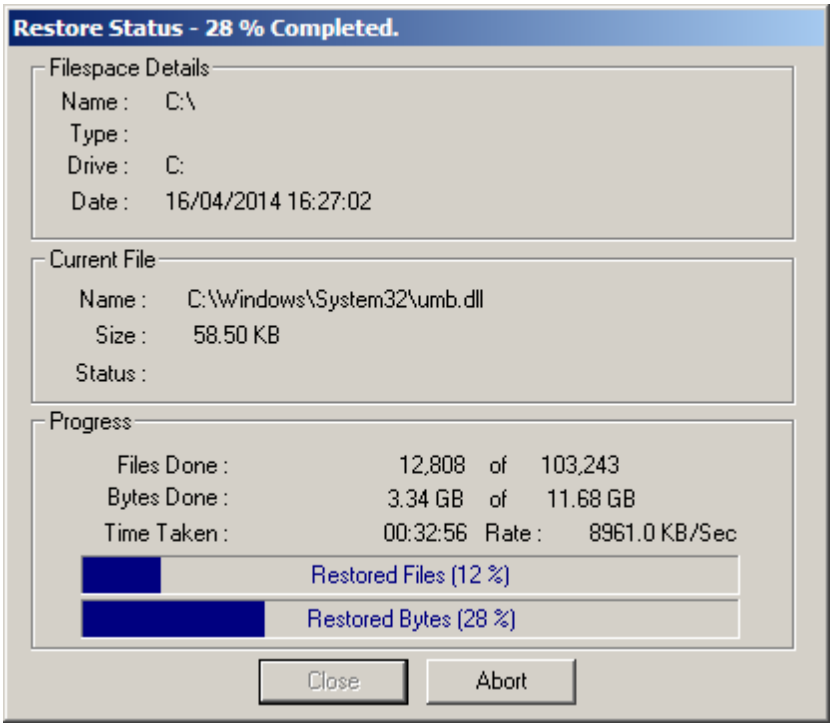

CBMR - Welcome
CBMR
Welcome to the CBMR Manual Recovery Wizard which gives greater control and flexibility in restoring your system.
Select the operation you want to do and select [Next] to proceed.
Access Configuration
Create Partitions and Volumes
Restore Files
Make Bootable
Dissimilar Hardware
< Back
Next >
Cancel

Press Next> to select which datasets to restore. Generally, each dataset represents a disk partition or volume. Put a tick against each dataset that should be restored:


CBMR - Select Datasets to Restore
At least one System and one Boot partition must be selected in order to recover your machine. This may be the same partition. You can select additional drives to be restored by ticking the check box next to the drive.
Drive Letter
Boot
Syst...
Name
File System
C: Yes C:\
E: E:\
F: F:\
G: G:\
H: H:\
I: I:\
J: J:\
K: K:\
L: L:\
M: M:\
Select All
Deselect All
< Back
Next >
Cancel

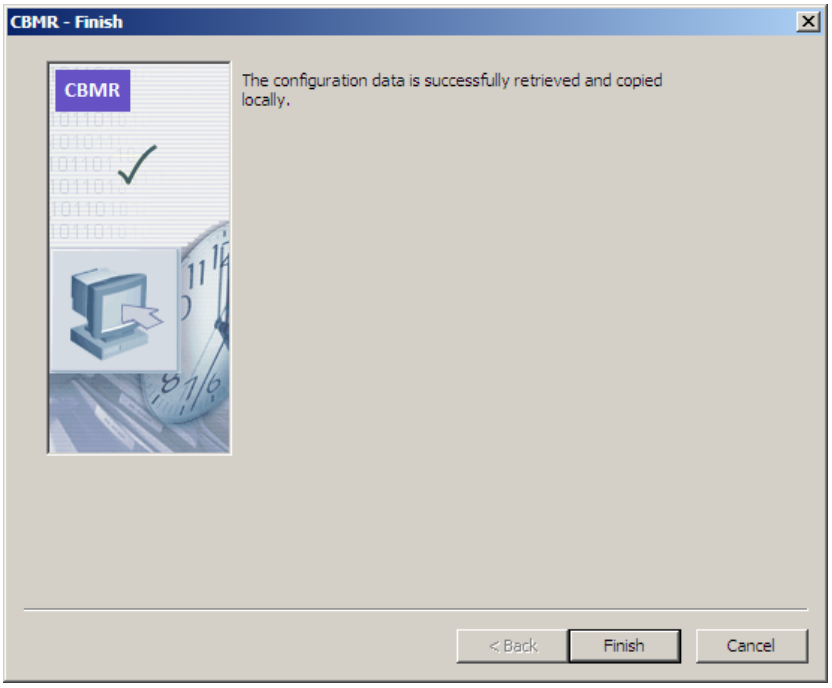
Press Next> to continue.

A new window appears containing the restore status of recovered files, with progress bars indicating how much of the backup has been restored. This display also shows the recovery statistics in terms of time, size and throughput.



This process may take some time if the backups are large. You may select the Abort button to terminate the file recovery process, but this may leave the disk or partition in an unpredictable state, which may render it unusable.

If any errors occur during the recovery, an error message will be shown in the window. Refer to the logs post recovery to establish the cause of any error. When the restore files step completes, select Close and the following dialogue is displayed:

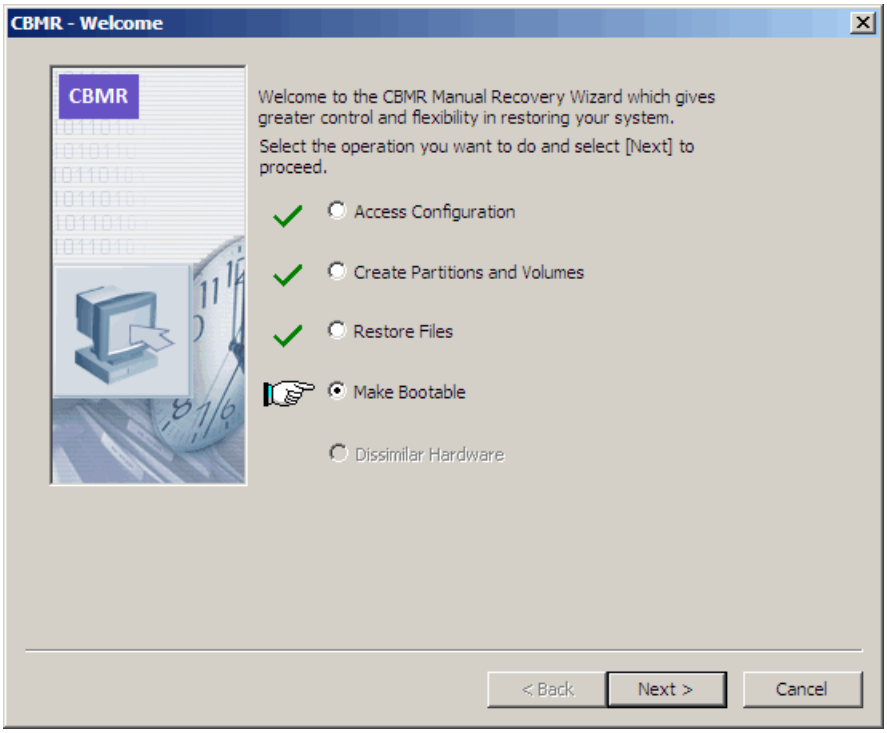


Select Finish to complete the step and return to the **Manual Recovery Wizard**

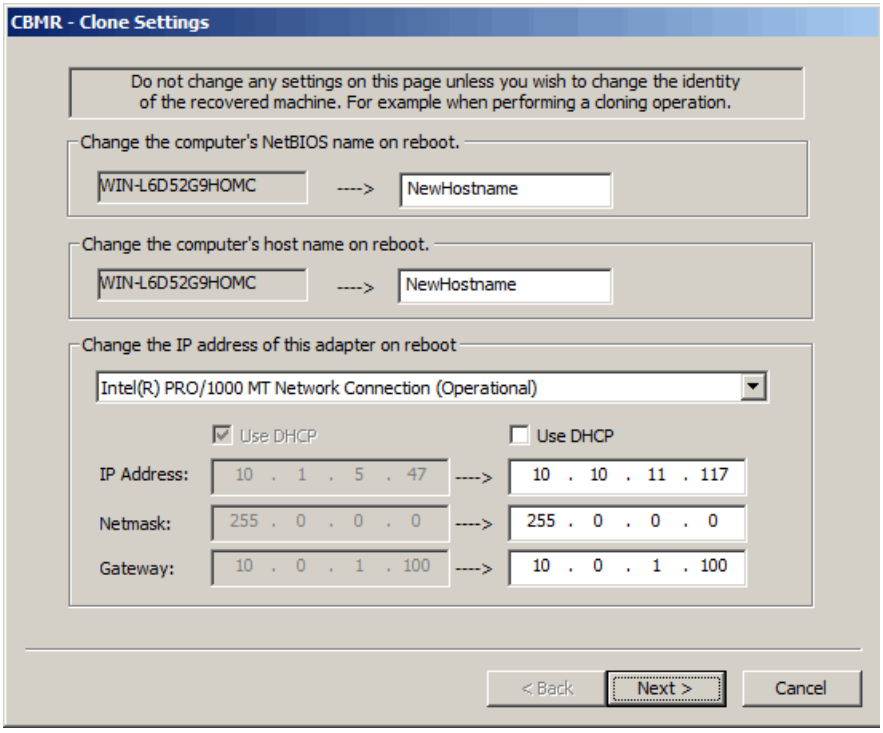
Copyright © 1998-2014 Cristie Software Ltd.

Make Bootable

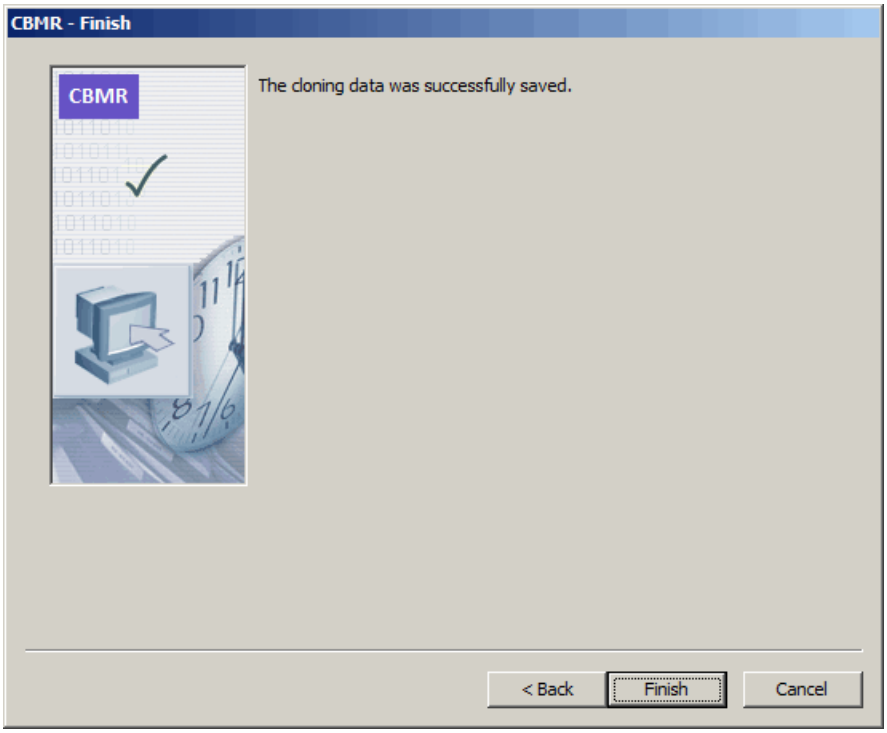
The next step in the manual recovery sequence is to make the original disk 'bootable'. This involves re-creating the MBR of the boot disk and modifying the registry with the new disk GUID.


CBMR - Welcome
CBMR
Welcome to the CBMR Manual Recovery Wizard which gives greater control and flexibility in restoring your system.
Select the operation you want to do and select [Next] to proceed.
Access Configuration
Create Partitions and Volumes
Restore Files
Make Bootable
Dissimilar Hardware
< Back
Next >
Cancel

Press Next> to commence the **Make Bootable** step. You will now be able to change the hostname and/or the machine's IP addresses on reboot.

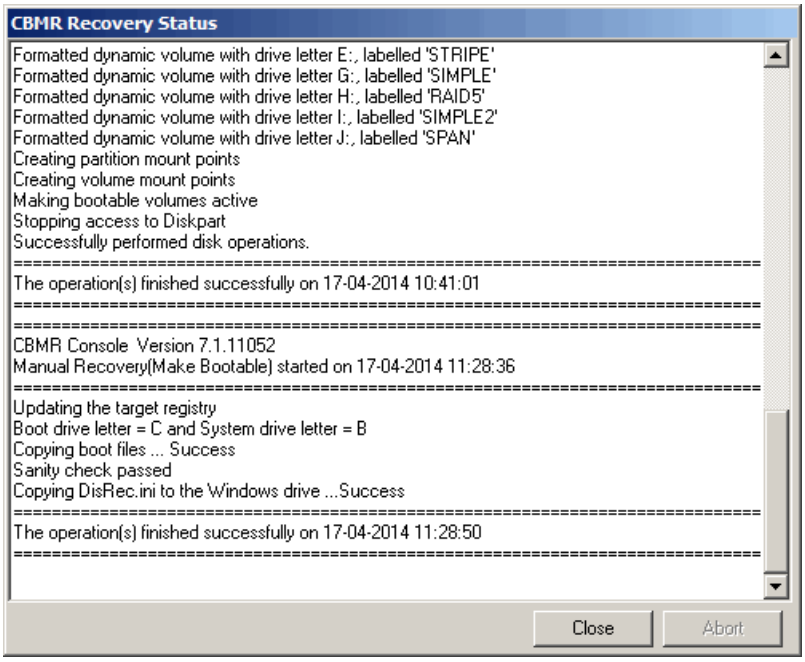

CBMR - Clone Settings
Do not change any settings on this page unless you wish to change the identity of the recovered machine. For example when performing a cloning operation.
Change the computer's NetBIOS name on reboot.
WIN-L6D52G9HOMC
---->
NewHostname
Change the computer's host name on reboot.
WIN-L6D52G9HOMC
---->
NewHostname
Change the IP address of this adapter on reboot
Intel(R) PRO/1000 MT Network Connection (Operational)
Use DHCP
Use DHCP
IP Address:
10 . 1 . 5 . 47
---->
10 . 10 . 11 . 117
Netmask:
255 . 0 . 0 . 0
---->
255 . 0 . 0 . 0
Gateway:
10 . 0 . 1 . 100
---->
10 . 0 . 1 . 100
< Back
Next >
Cancel

If no hostname or IP change is required, click Next> to continue. The cloning data is confirmed with the following dialogue.



Click Finish to complete the Make Bootable step.

A new dialogue window opens summarising the success or failure of the operation:

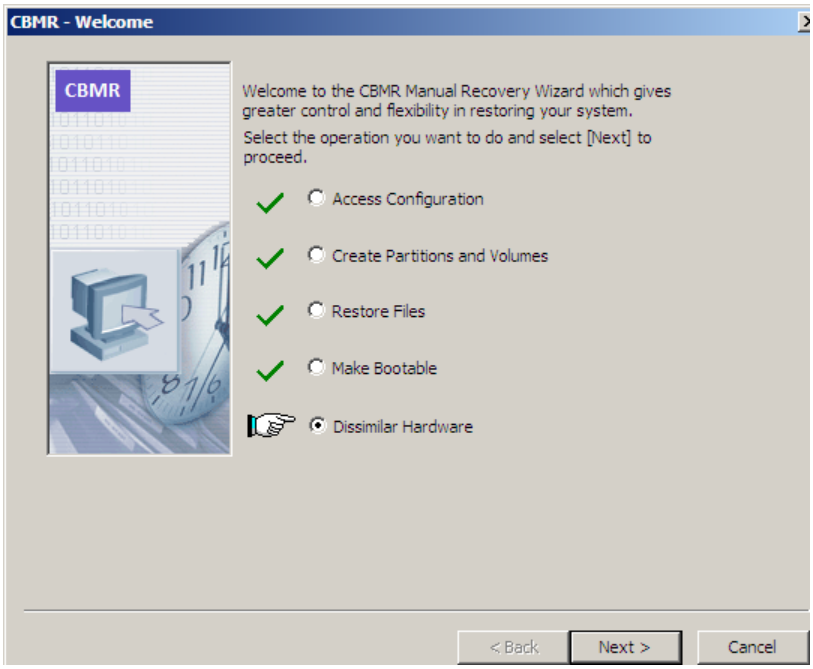

CBMR Recovery Status
Formatted dynamic volume with drive letter E:, labelled 'STRIPE'
Formatted dynamic volume with drive letter G:, labelled 'SIMPLE'
Formatted dynamic volume with drive letter H:, labelled 'RAID5'
Formatted dynamic volume with drive letter I:, labelled 'SIMPLE2'
Formatted dynamic volume with drive letter J:, labelled 'SPAN'
Creating partition mount points
Creating volume mount points
Making bootable volumes active
Stopping access to Diskpart
Successfully performed disk operations.
The operation(s) finished successfully on 17-04-2014 10:41:01
CBMR Console Version 7.1.11052
Manual Recovery(Make Bootable) started on 17-04-2014 11:28:36
Updating the target registry
Boot drive letter = C and System drive letter = B
Copying boot files ... Success
Sanity check passed
Copying DisRec.ini to the Windows drive ...Success
The operation(s) finished successfully on 17-04-2014 11:28:50
Close
Abort

Press Close to complete the step and return to the **Manual Recovery Wizard**.

Copyright © 1998-2014 Cristie Software Ltd.

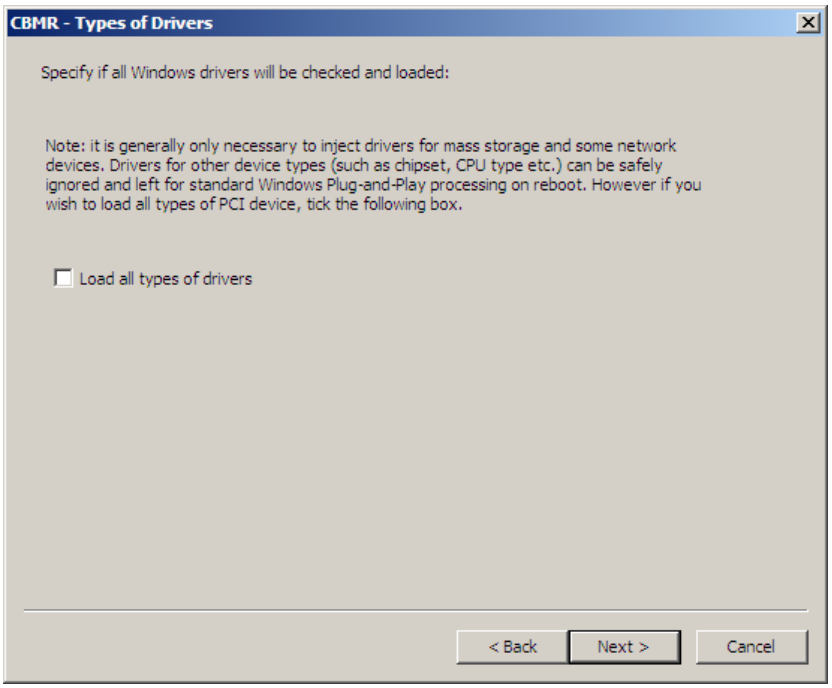
Dissimilar Hardware

The final step in the manual DR sequence is to check if the recovery is to **Dissimilar Hardware**.

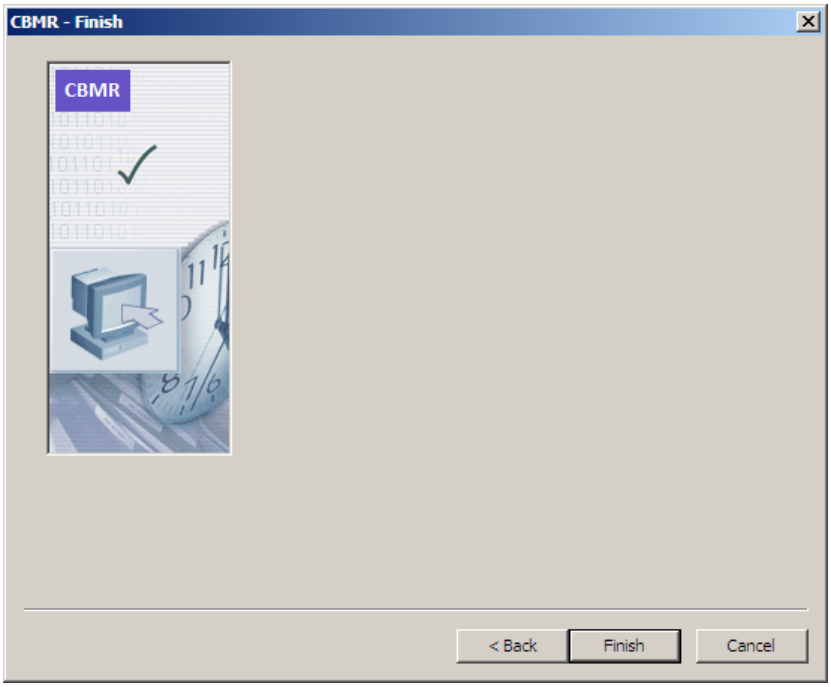

CBMR - Welcome
CBMR
Welcome to the CBMR Manual Recovery Wizard which gives greater control and flexibility in restoring your system.
Select the operation you want to do and select [Next] to proceed.
Access Configuration
Create Partitions and Volumes
Restore Files
Make Bootable
Dissimilar Hardware
< Back
Next >
Cancel

This is determined by comparing the drivers currently in use by WinPE2 or WinPE4 and the drivers listed in the recovered machine's registry.

The step first prompts for what driver types should be checked. By default, only **Mass Storage** (disk) and **network devices** are checked.


CBMR - Types of Drivers
Specify if all Windows drivers will be checked and loaded:
Note: it is generally only necessary to inject drivers for mass storage and some network devices. Drivers for other device types (such as chipset, CPU type etc.) can be safely ignored and left for standard Windows Plug-and-Play processing on reboot. However if you wish to load all types of PCI device, tick the following box.
Load all types of drivers
< Back
Next >
Cancel

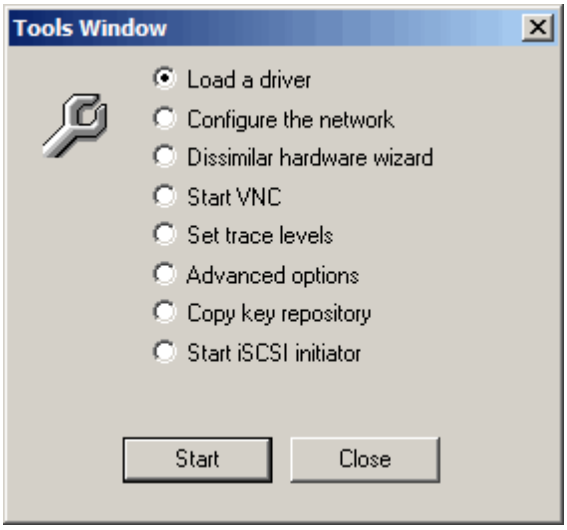
Press Next> to continue. For recovery to similar hardware, no new devices will be found and this will be confirmed by this dialogue:



Press Finish to complete the manual recovery sequence.

3.4.2.4 Tools

There are a number of tools that can assist with the recovery process. They are all collected under this command button:



The options available are:

- Load a driver
- Configure the network
- Dissimilar Hardware Wizard
- Start VNC
- Set trace levels
- Copy key repository

Copyright © 1998-2014 Cristie Software Ltd.

- Advanced options
- Start iSCSI initiator

Load a driver allows a new mass storage or NIC driver to be injected into the running booted WinPE2 or WinPE4 DR environment. This would be used, for example, to support a mass-storage (disk) device not currently supported out-of-box. This should be done prior to starting the DR sequence.

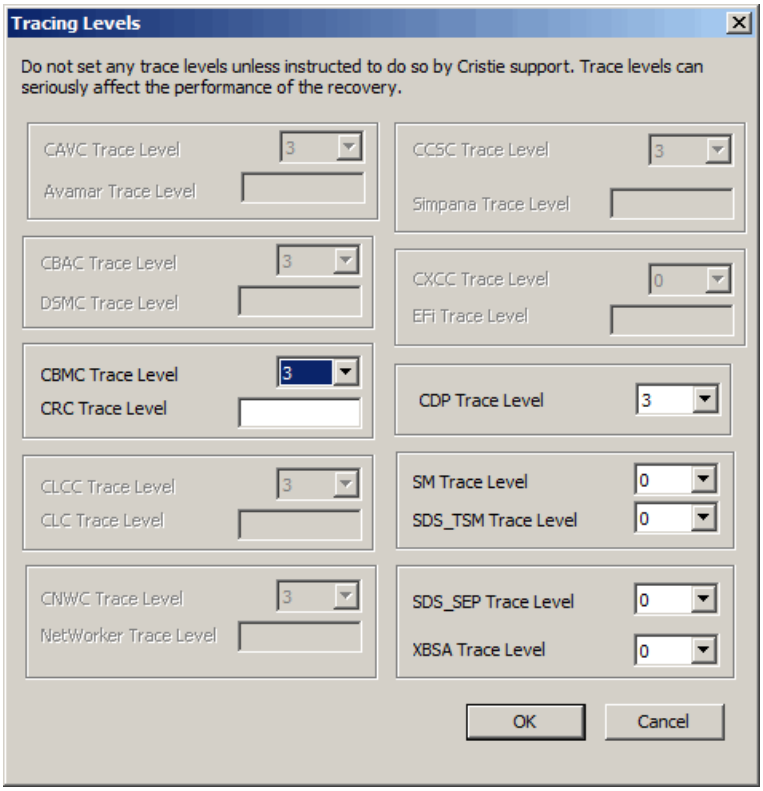
Selecting **Configure the network** will start the **Cristie Network Configurator** tool. This provides extensive facilities to configure networks during the DR process.

The **Dissimilar Hardware Wizard** will allow drivers to be injected into the recovered system when the target hardware has different devices from the original (eg. RAID controllers). Normally, this will be done automatically as part of the DR sequence and will not need to be run manually.

Start VNC will run a VNC server within the WinPE2 or WinPE4 environment, allowing external VNC clients to remotely connect during the DR session. The start process will provide you with the current IP address of the WinPE2 or WinPE4 environment, which you will need to specify in the VNC client.

> ***Note: the VNC connection is also password protected. The VNC feature is intended for diagnosing DR problems under the guidance of Cristie Support, who will provide the password upon request.***

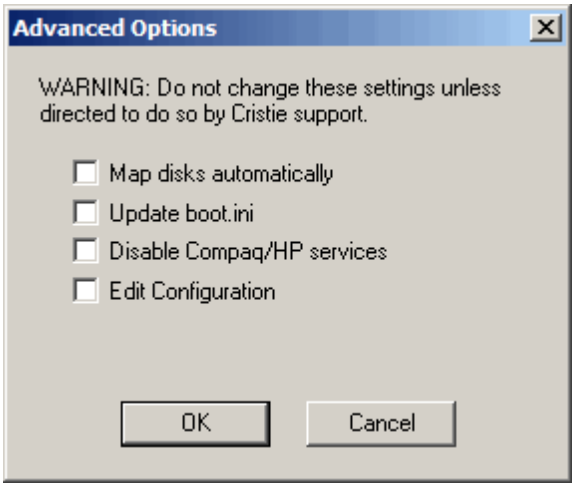
Set trace levels allows the DR log file trace to be increased or decreased as required:



It is recommended that the trace levels are only changed when advised to do so by Cristie Support staff. This is because they could have a severe impact upon the performance of the backup restore process.

Copy key repository used to define a key repository path.

Advanced Options should only be selected when advised to do so by Cristie Support staff.



Start iSCSI initiator - please contact Cristie Support if you wish to use this feature.

Cristie Network Configurator Tool

The **Cristie Network Configurator** tool provides extensive facilities to configure the network during the recovery process. It offers the following features:

- supports multiple NICs
- configure individual NIC parameters for duplex mode and link speed
- the ability to select DHCP allocated or static IP addresses
- the ability to setup DNS server IP addresses
- the ability to setup the Network Identification of the recovering system
- allow file shares to be set on the recovering system
- map/unmap network drives

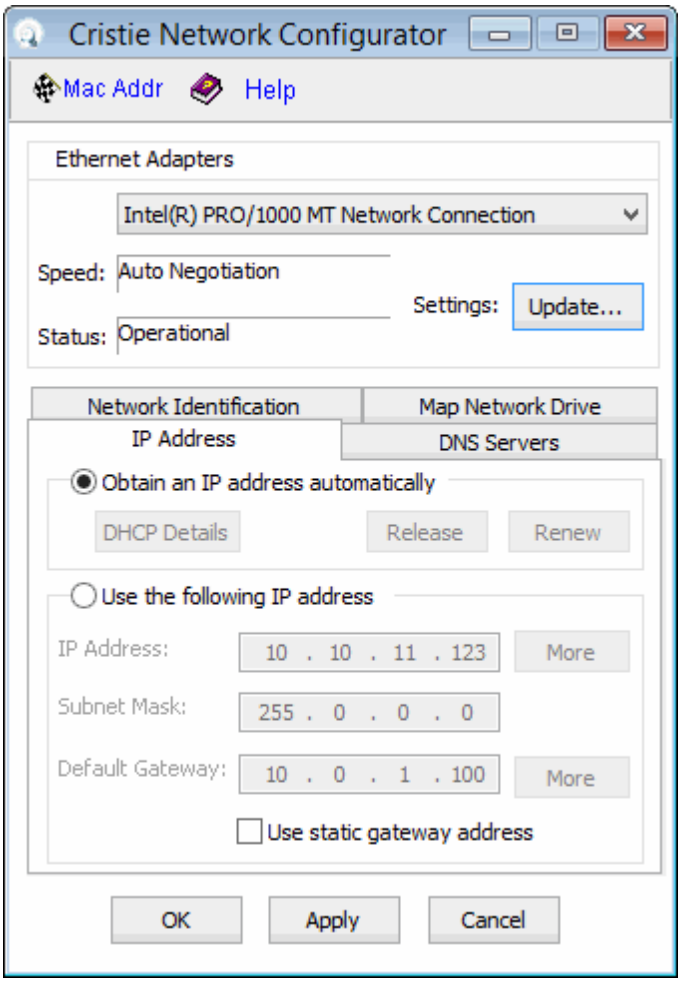
Select the

button at the top of the dialogue to show Network Configurator online help.

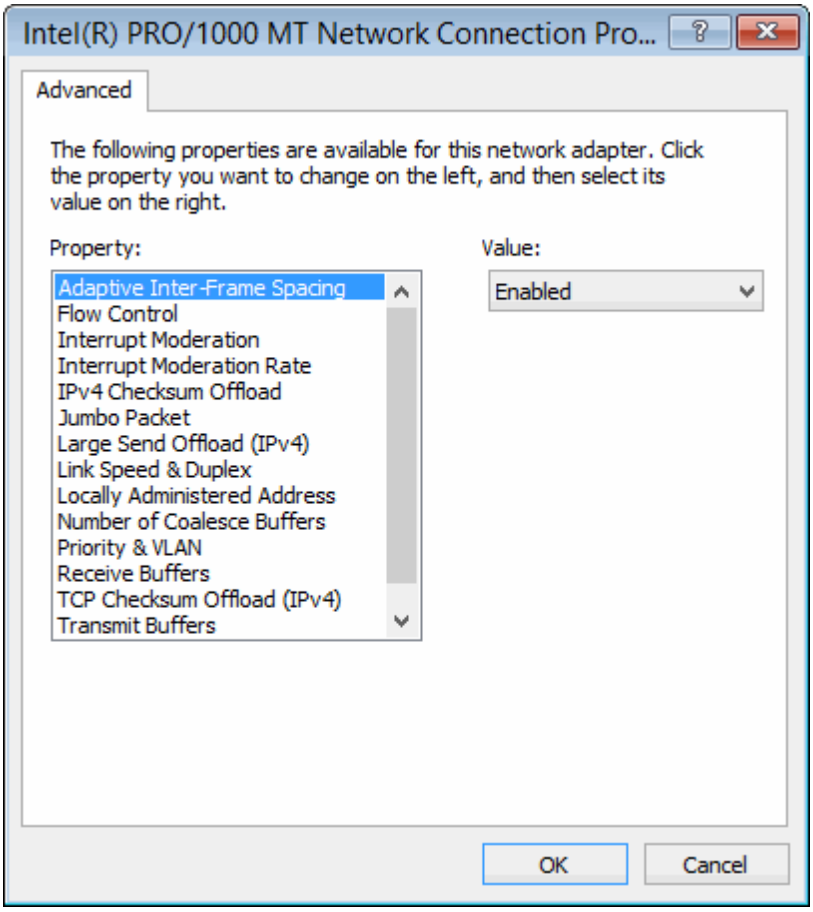
Copyright © 1998-2014 Cristie Software Ltd.

Configure NIC Parameters

It is possible to change both the link speed and duplex mode for any NIC detected on the recovering target system. Select the desired NIC (there could be more than one) from the drop down box and then select Update....

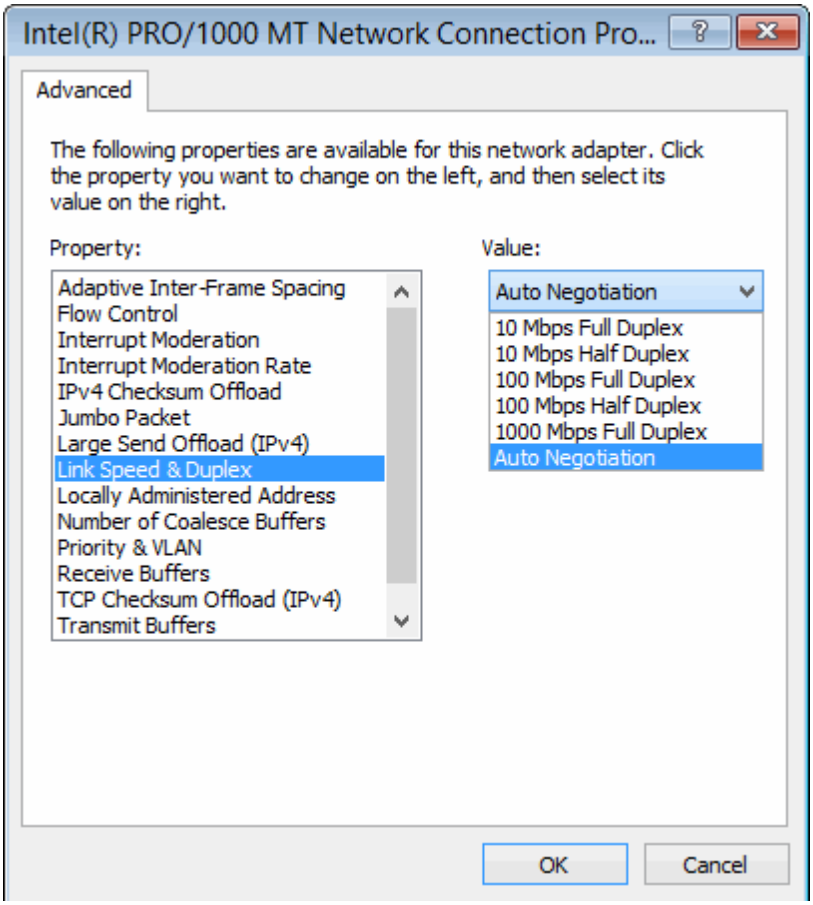


The resulting display offers numerous NIC properties that can be changed. This property list is dependent upon the NIC - ie. not all properties will be available for all NICs.



To change the NIC speed or duplex setting, select the corresponding *Property* from the dialogue and then select the required value from the *Value* drop down box as shown below:

Copyright © 1998-2014 Cristie Software Ltd.



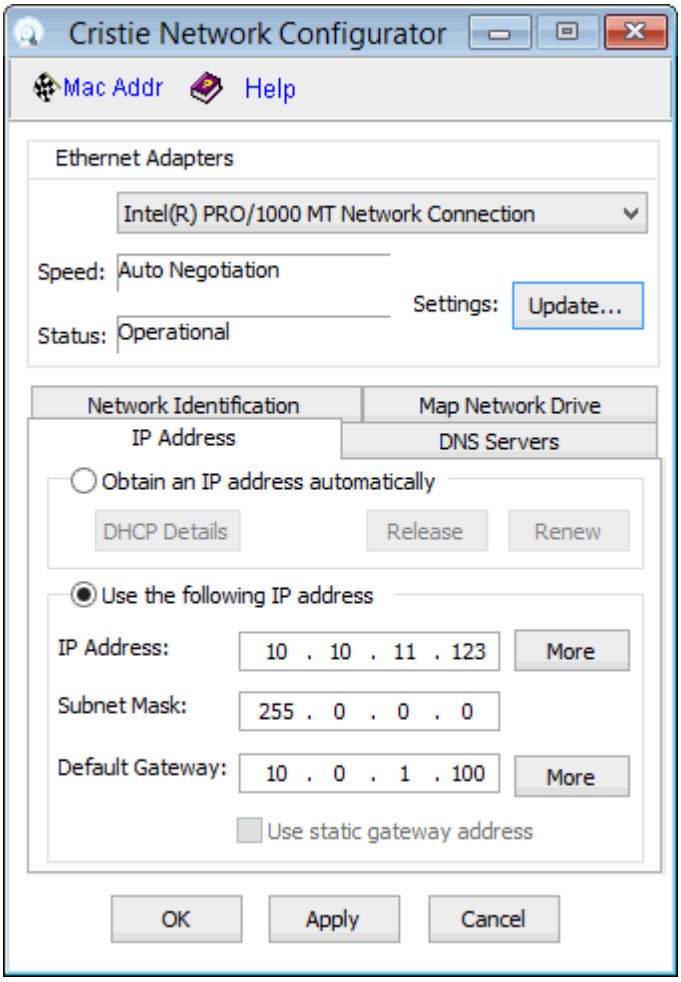
Again, note that the speed/duplex settings available are NIC dependent. *Auto Negotiation* is generally the NIC default setting. Other NIC properties may be changed as required.

If the NIC is currently connected to the network then the *Status* will be shown as **Operational**. Otherwise the NIC is considered to be **Non-Operational**.

Assign Static or DHCP IP Settings

Normally the WinPE2 or WinPE4 DR environment will start with DHCP enabled and active. However, if a static IP is required, use the 'Use the following IP address' option to manually configure.

First ensure the desired network adapter is selected from the drop down list. If a static IP address is to be applied, select the 'Use the following IP address' button. This will automatically deselect the default DHCP option and allow the static IP parameters to be defined.



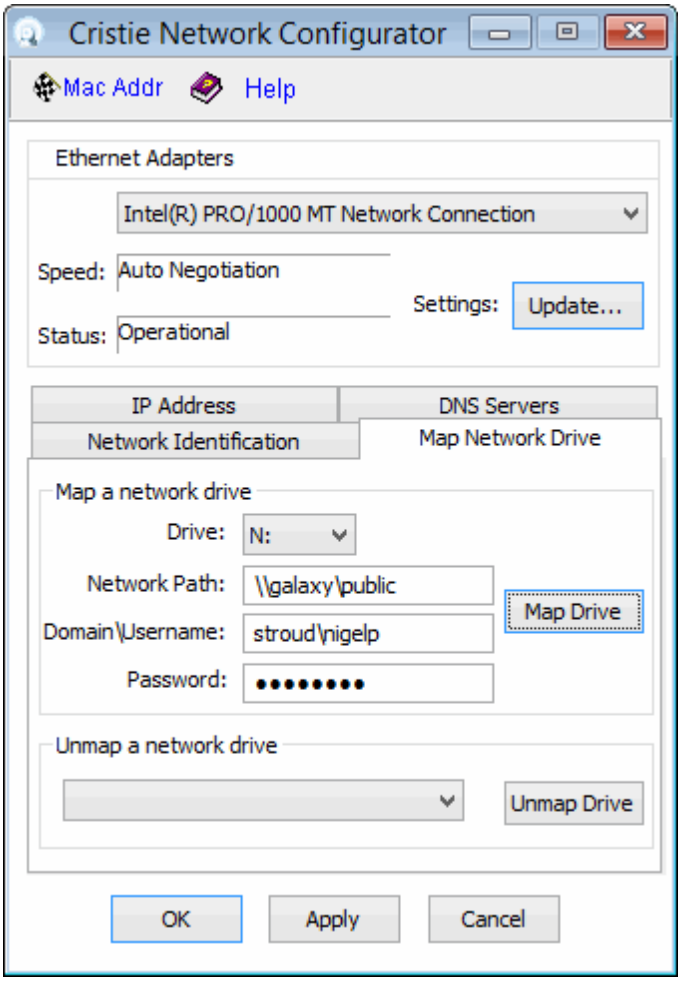
Set the new IP address, subnet mask and gateway IP address. The More button will allow the system to have more than one static IP address. Click on Apply to confirm the settings for the selected adapter.

This feature will also allow the DHCP lease to be released or renewed, as required.

Map a Network Drive

In order to simplify access to network resources, the Network Configurator allows you to map a network drive to a network share. Start the Cristie Network Configurator from the **Tools** menu and select the **Map Network Drive** tab.

Copyright © 1998-2014 Cristie Software Ltd.

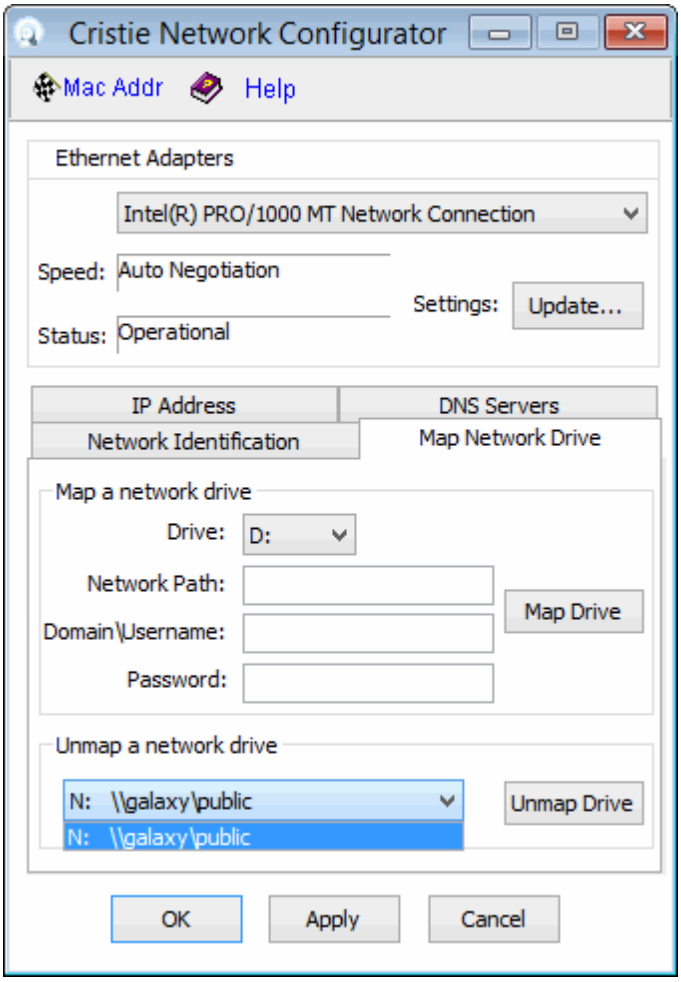


Select the drive letter that you wish to allocate from the **Drive** drop-down box and type in the share name that you wish to associate with it. Also specify the network credentials to be used to access the share.

Press Map Drive to confirm the share operation. If successful, the share will be added to the **Unmap a network drive** drop down list.

Disconnect Network Drives

If you need to disconnect a mapped drive for any reason, this option allows you to do this. Just select the drive that you wish to disconnect from the Unmap a network drive drop down list and then click Unmap Drive.



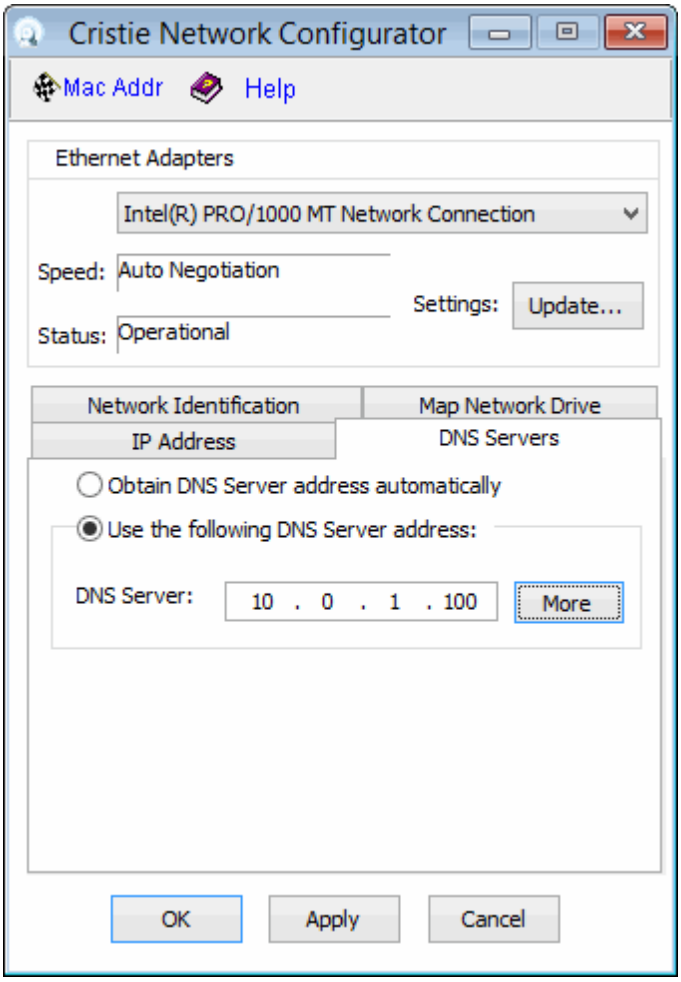
The mapped drive is removed from the list to confirm the operation.

Setup DNS Servers

DNS server IP addresses are automatically set when the WinPE2 or WinPE4 DR environment boots. However, options are provided to allow DNS server IP addresses to be manually set if required.

> ***Note: WINS servers are not currently supported by this tool.***

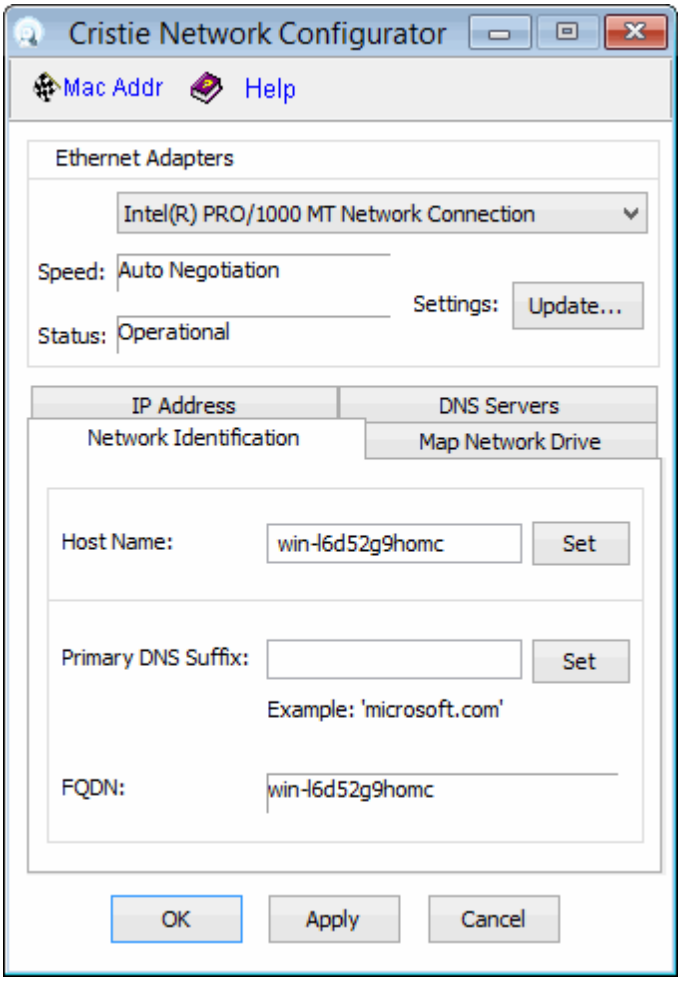
Copyright © 1998-2014 Cristie Software Ltd.



Select the **'Use the following DNS Server address'** radio button and enter the new DNS IP server address. If required, select the More button to add several DNS IP addresses. Press Apply to activate the new address.

Setup Network Identification

Click the **Network Identification** tab to setup a new hostname for the recovering system. This allows the WinPE2 or WinPE4 hostname and Primary DNS suffix to be changed during a DR session if required. These details are transient and only apply only while theWinPE2 or WinPE4 DR session is running. They are not applied to the recovered system when it reboots after the DR session.



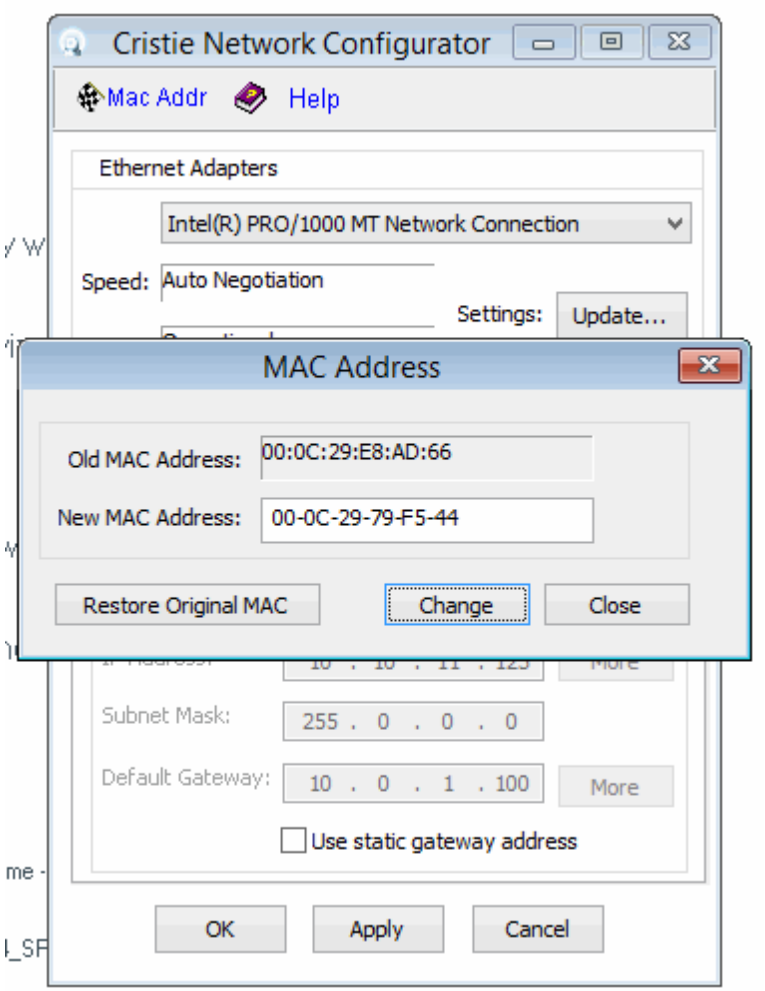
Enter the new Computer Name and press Set to confirm the change.

Display MAC Address

It is possible to display and change the local MAC address of the recovering system. Select the MAC Address

button at the top of the Main menu dialogue:

Copyright © 1998-2014 Cristie Software Ltd.



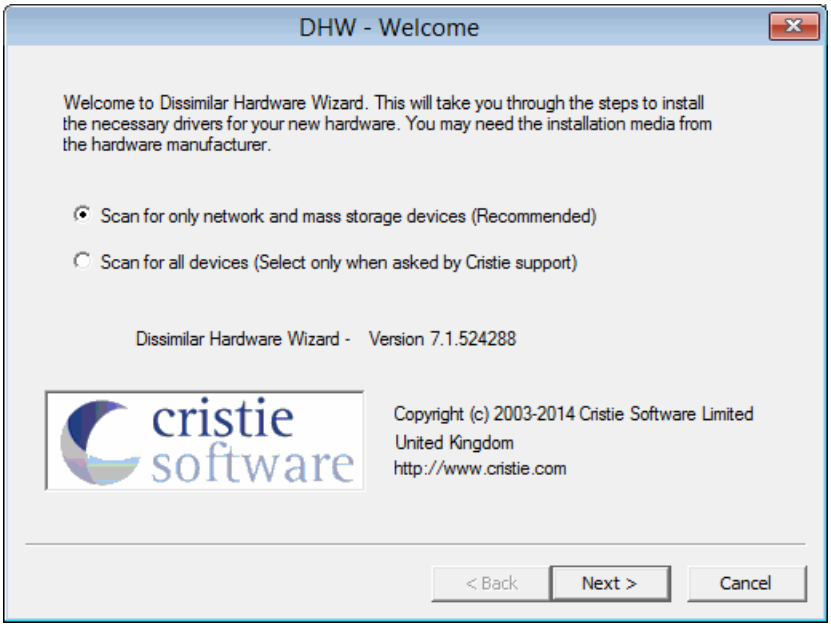
Change the MAC address by entering a new value in the form xx-xx-xx-xx-xx-xx and selecting Change. The original MAC address will be preserved and can be restored using the Restore Original MAC button.

Dissimilar Hardware Wizard

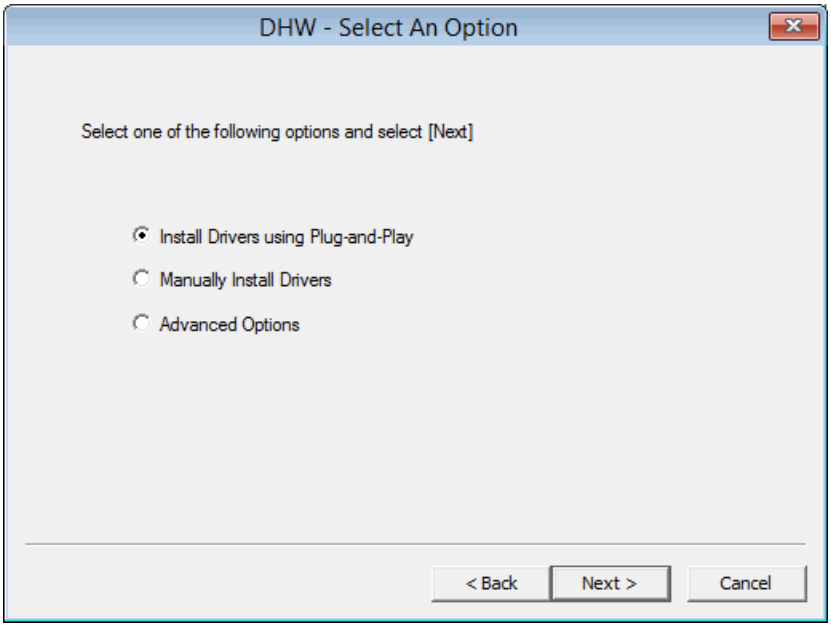
A restore to dissimilar hardware is normally detected during the Automatic or Manual DR sequence. Drivers will be injected automatically at the end of the restore sequence if a source location has been provided. However, if this process has failed for some reason, or additional drivers are required to be injected into the recovering machine, then this **Dissimilar Hardware Wizard** (DHW) tool is provided.

> ***Note: it is only necessary to load the drivers for the hard disk, NIC and, rarely, the HAL. Drivers for the hard disks and NIC can be determined by Plug-and-Play (PnP) and may be readily identified. However, changes required in the CPU model via a change in HAL cannot yet be determined by PnP - these need to be loaded manually.***

If you wish to scan for just Mass Storage and Network devices (the minimum required to boot a dissimilar system), select Next> to continue to the next step of the Wizard. This is the recommended option. Under the guidance of **Cristie Support**, you may be asked to scan for all devices. In this case, tick the **'Scan for all devices'** box before selecting Next>.


DHW - Welcome
Welcome to Dissimilar Hardware Wizard. This will take you through the steps to install the necessary drivers for your new hardware. You may need the installation media from the hardware manufacturer.
Scan for only network and mass storage devices (Recommended)
Scan for all devices (Select only when asked by Cristie support)
Dissimilar Hardware Wizard - Version 7.1.524288
cristie software
Copyright (c) 2003-2014 Cristie Software Limited
United Kingdom
http://www.cristie.com
< Back
Next >
Cancel

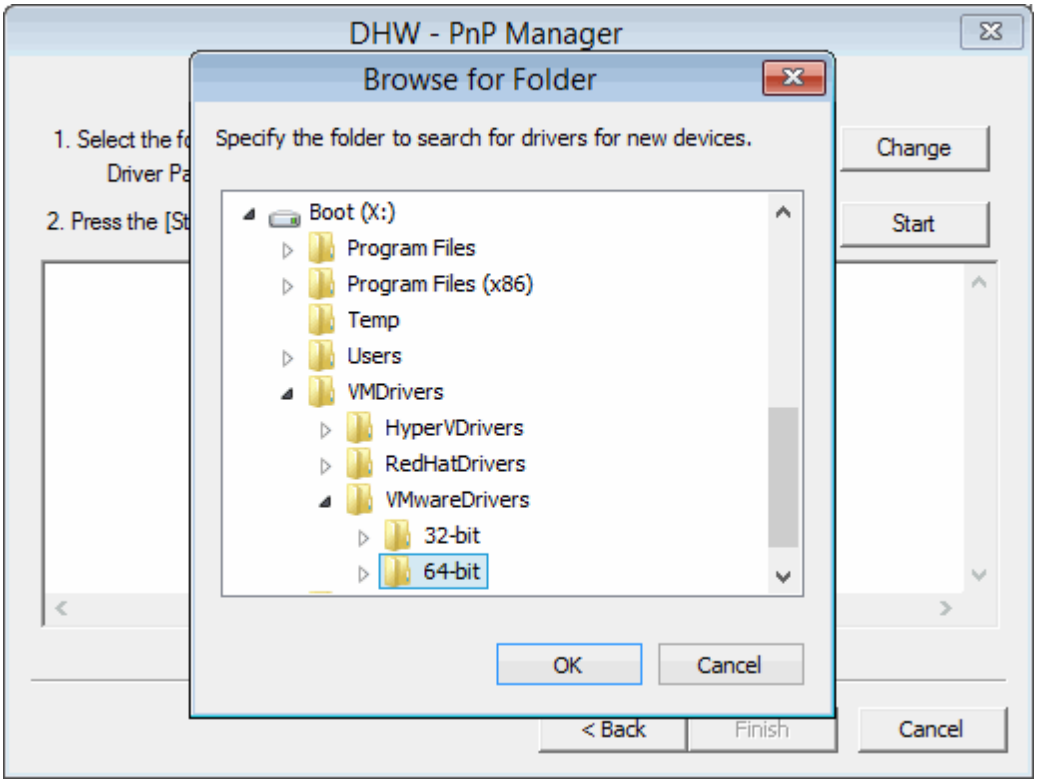
Select the **'Install Drivers using Plug-and-Play'** option:


DHW - Select An Option
Select one of the following options and select [Next]
Install Drivers using Plug-and-Play
Manually Install Drivers
Advanced Options
< Back
Next >
Cancel

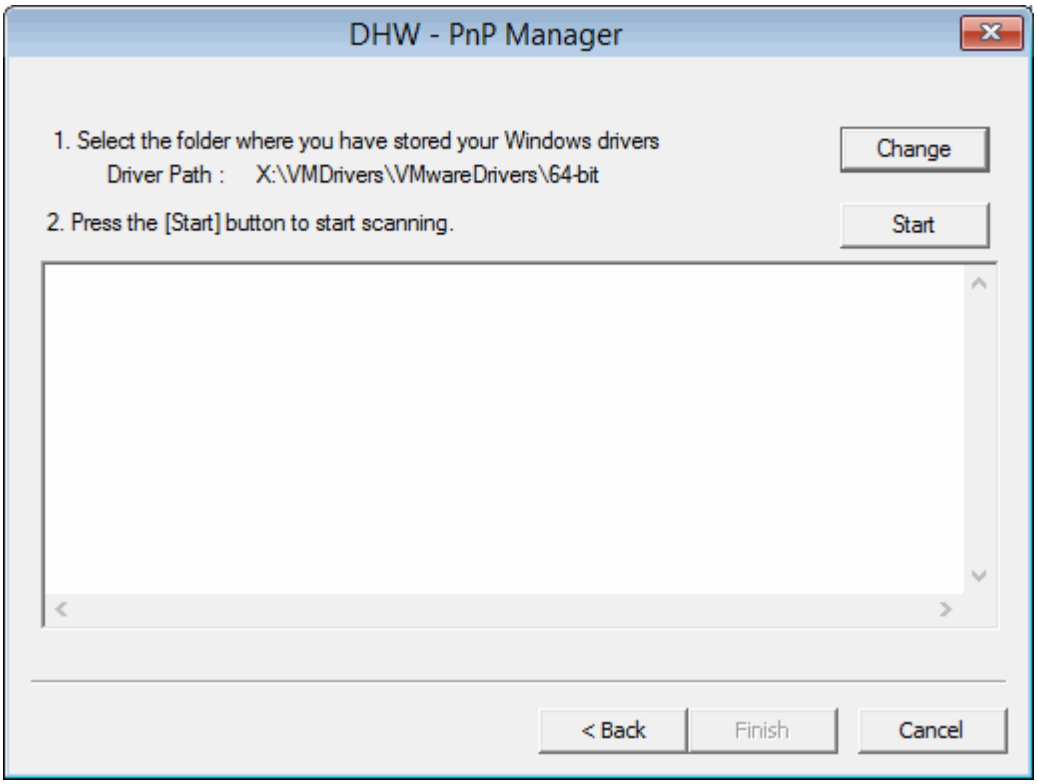
Install Drivers using Plug-and-Play

The window appears empty to start with. The set of drivers located on the recovery CD is the default choice, but in practice they should not be used. Instead, change the driver search path to where you have actually located your drivers (for example, to a network share or another CD) with the **Change** command button.

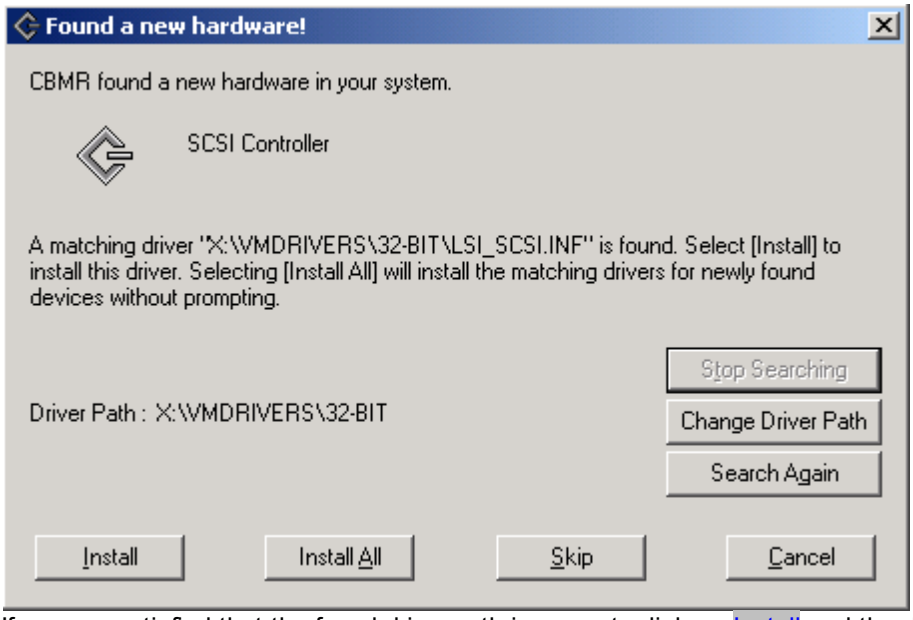
Copyright © 1998-2014 Cristie Software Ltd.



In the example above, the driver search path is changed to the VMware drivers on the WinPE boot CD. Begin the PnP driver detection by clicking Start.



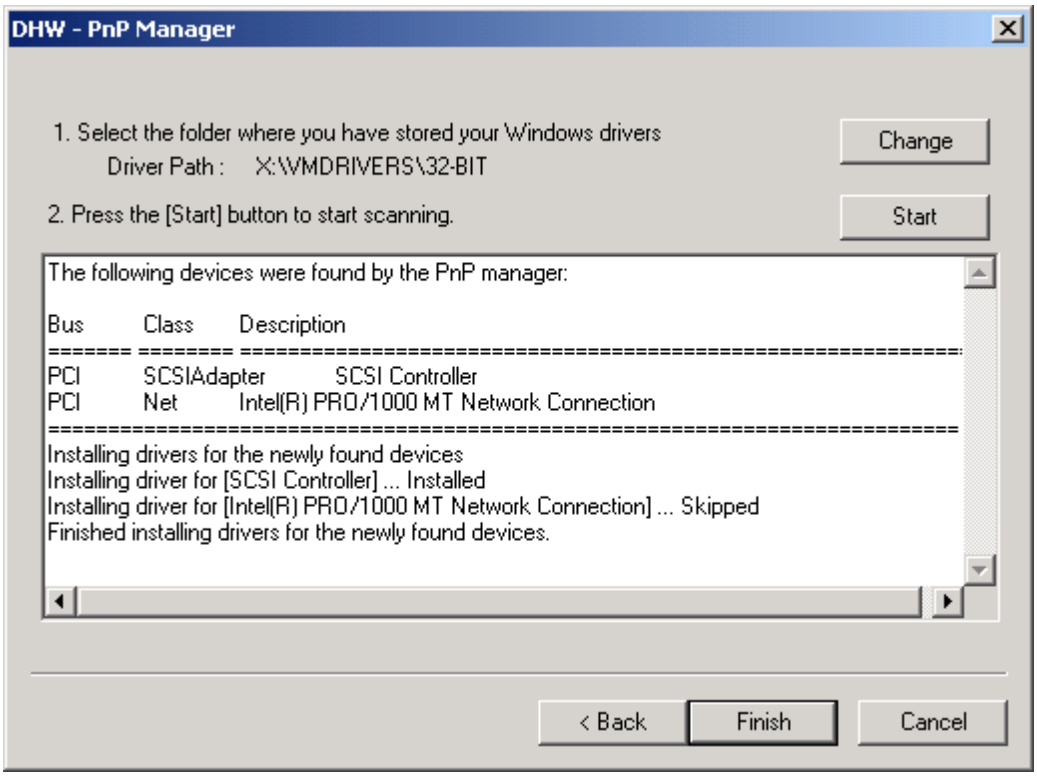
The process checks the devices that it can detect and when it finds one that does not have a driver loaded, it will offer to install it. The example below shows an LSI SCSI device being detected:


Found a new hardware!
CBMR found a new hardware in your system.
SCSI Controller
A matching driver "X:\VMDRIVERS\32-BIT\LSI_SCSI.INF" is found. Select [Install] to install this driver. Selecting [Install All] will install the matching drivers for newly found devices without prompting.
Stop Searching
Driver Path : X:\VMDRIVERS\32-BIT
Change Driver Path
Search Again
Install
Install All
Skip
Cancel

If you are satisfied that the found driver path is correct, click on Install and the driver will be installed. The device scan will continue and may find, for example, other mass storage or network devices. Follow the steps above to install.

Drivers are usually .sys files. The .inf files define which driver files need to be loaded for a given device. You may need to confirm the location of the driver files for each device, or possibly find the path where they are stored. When you have the correct path, click on OK and the Wizard will look for more.

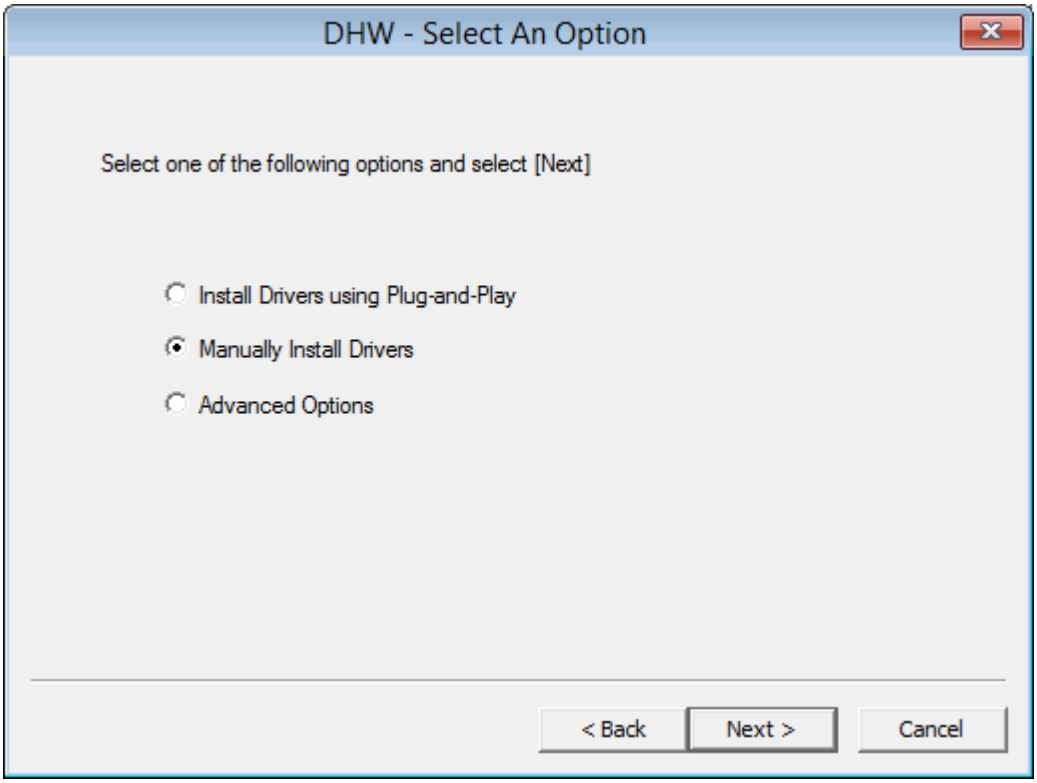
Once all of the drivers of the detected devices have been processed, the Wizard will indicate that the installation has finished. Click on Finish to proceed.


DHW - PnP Manager
1. Select the folder where you have stored your Windows drivers
Driver Path : X:\VMDRIVERS\32-BIT
Change
2. Press the [Start] button to start scanning.
Start
The following devices were found by the PnP manager:
Bus Class Description
PCI SCSIAdapter SCSI Controller
PCI Net Intel(R) PRO/1000 MT Network Connection
Installing drivers for the newly found devices
Installing driver for [SCSI Controller] ... Installed
Installing driver for [Intel(R) PRO/1000 MT Network Connection] ... Skipped
Finished installing drivers for the newly found devices.
< Back
Finish
Cancel

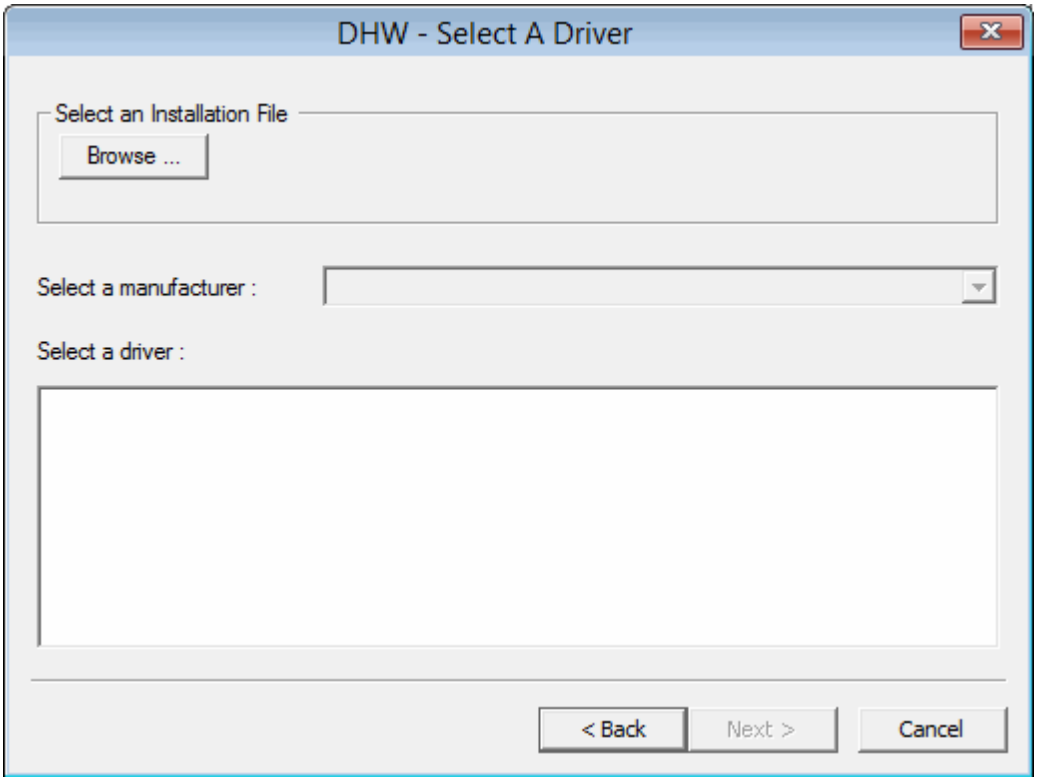
Manual Installation

Copyright © 1998-2014 Cristie Software Ltd.

Typically, you would only manually install a driver for a CPU/HAL change. Select **'Manually Install Drivers'** from the option menu:

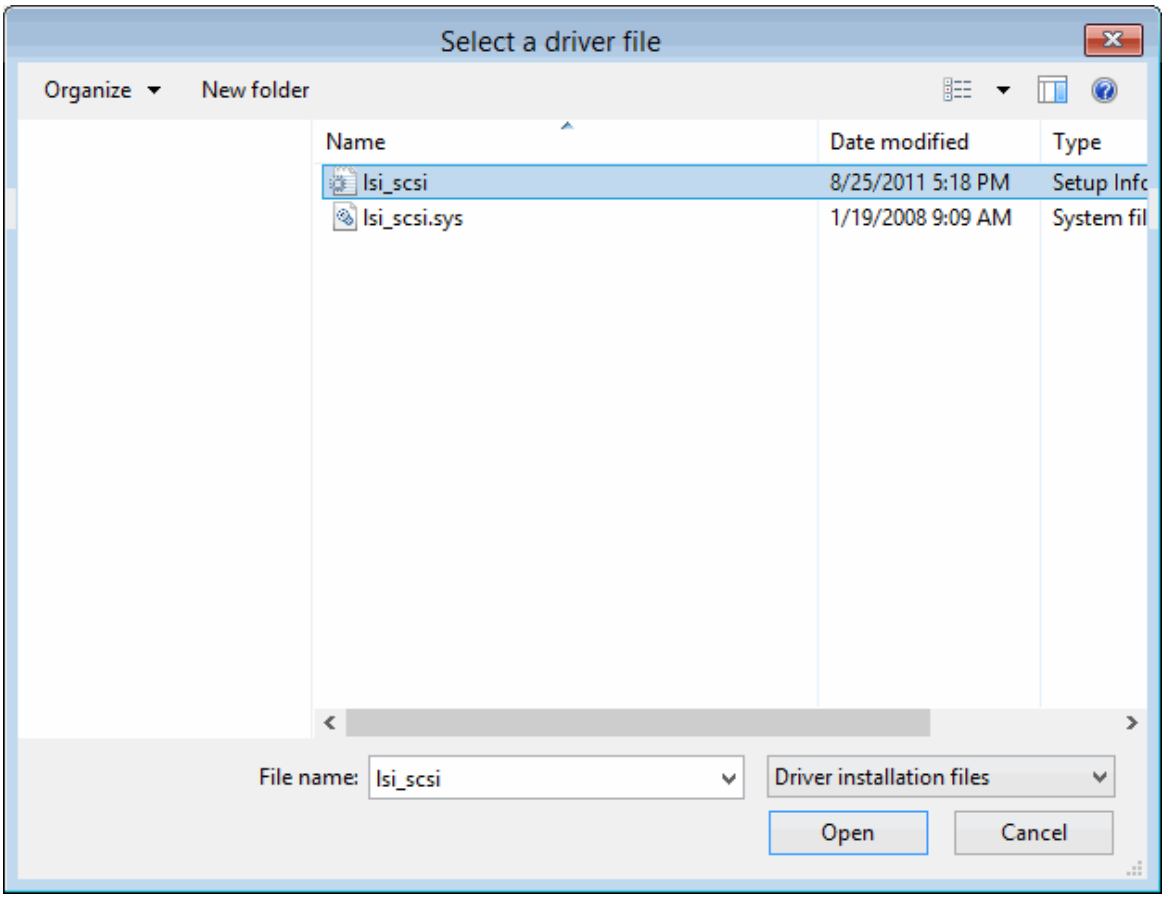

DHW - Select An Option
Select one of the following options and select [Next]
Install Drivers using Plug-and-Play
Manually Install Drivers
Advanced Options
< Back
Next >
Cancel

Then select Next>.

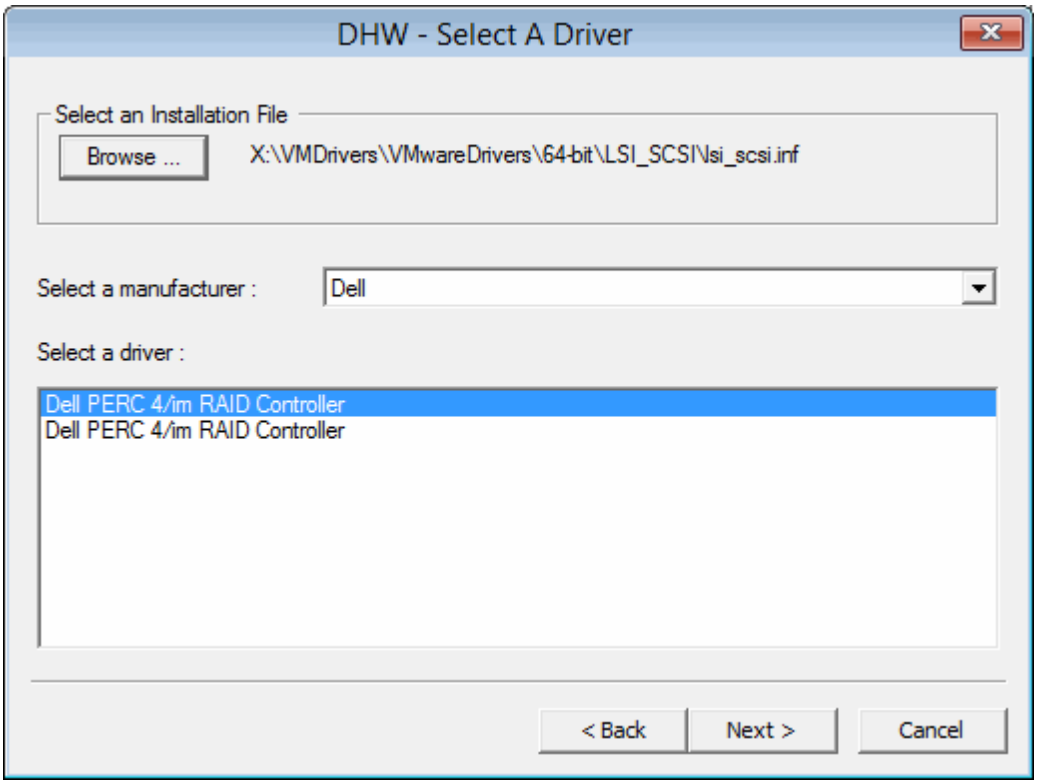


Select Browse... to locate the driver or HAL file you need by browsing to the appropriate folder that holds the .inf file. If you need to load the driver from another machine, then you can browse to a

share on that machine and then to the appropriate folder.

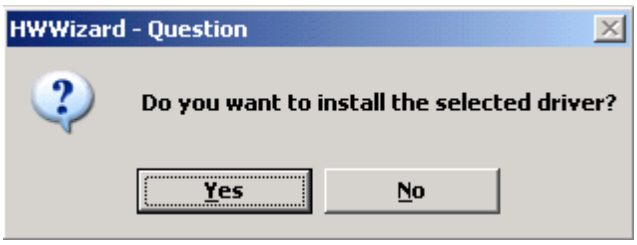


Here we are selecting the VMware SCSI controller driver:



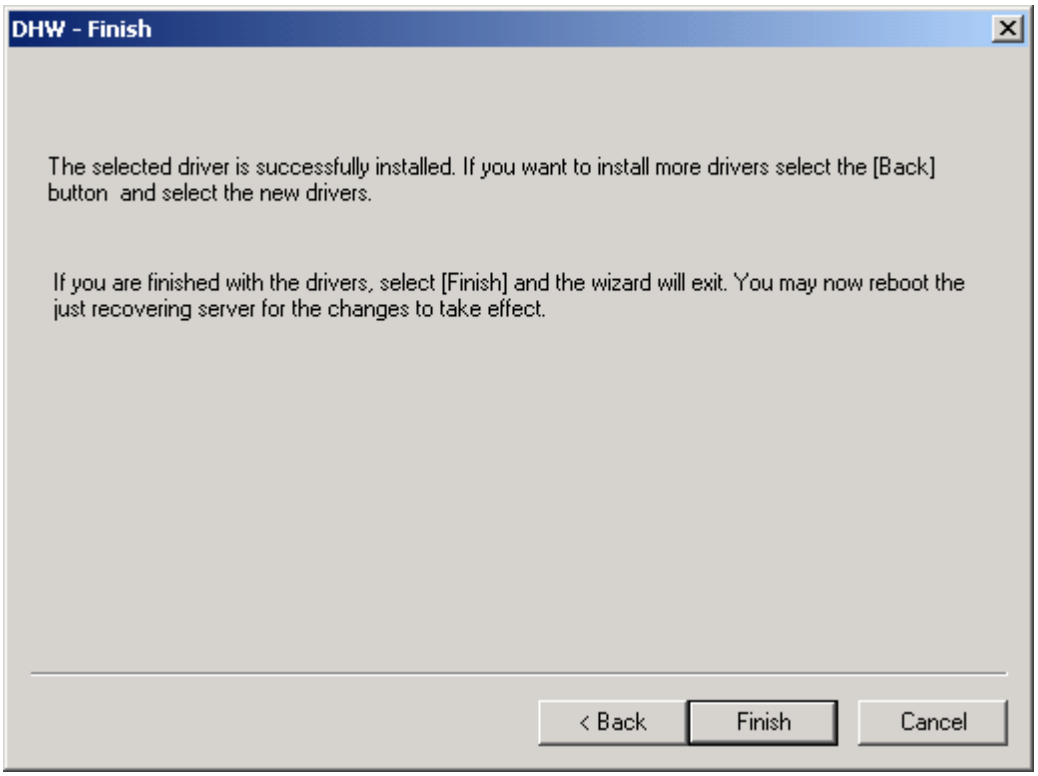
Copyright © 1998-2014 Cristie Software Ltd.

The Wizard allows you to select drivers that are grouped by manufacturer. Select the actual driver that you wish to install and click Next>.



After you confirm the selection, the Wizard determines which files need to be installed. You are given the opportunity to change the location from which they are loaded if required..

When the drivers have been installed, the Wizard allows you to go back to install another device driver or Finish the process.

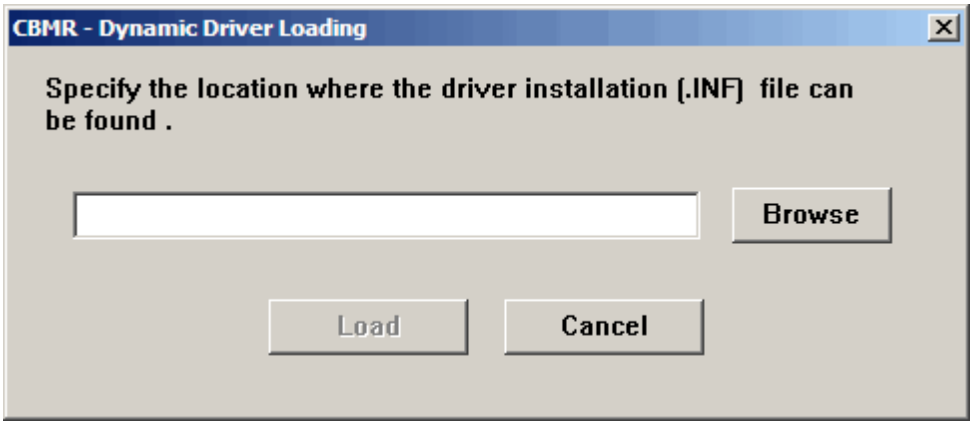

DHW - Finish
The selected driver is successfully installed. If you want to install more drivers select the [Back] button and select the new drivers.
If you are finished with the drivers, select [Finish] and the wizard will exit. You may now reboot the just recovering server for the changes to take effect.
< Back
Finish
Cancel

Load a Driver

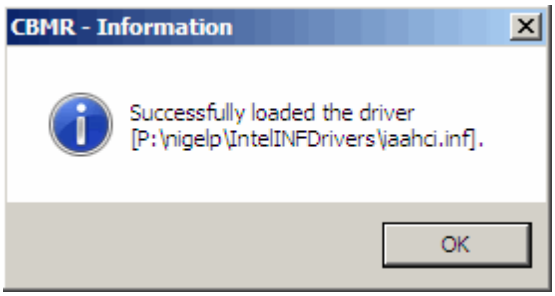
This option allows a **new mass storage** or **Network card driver** to be loaded into the WinPE2 or WinPE4 environment. Use this when WinPE2 or WinPE4 does not have a built-in driver for your hardware.

For example, if the DR environment does not show any disks to be recovered, you can inject a new mass storage device driver for the device and retry the DR Wizard.

You will be prompted for the location of the driver INF file:

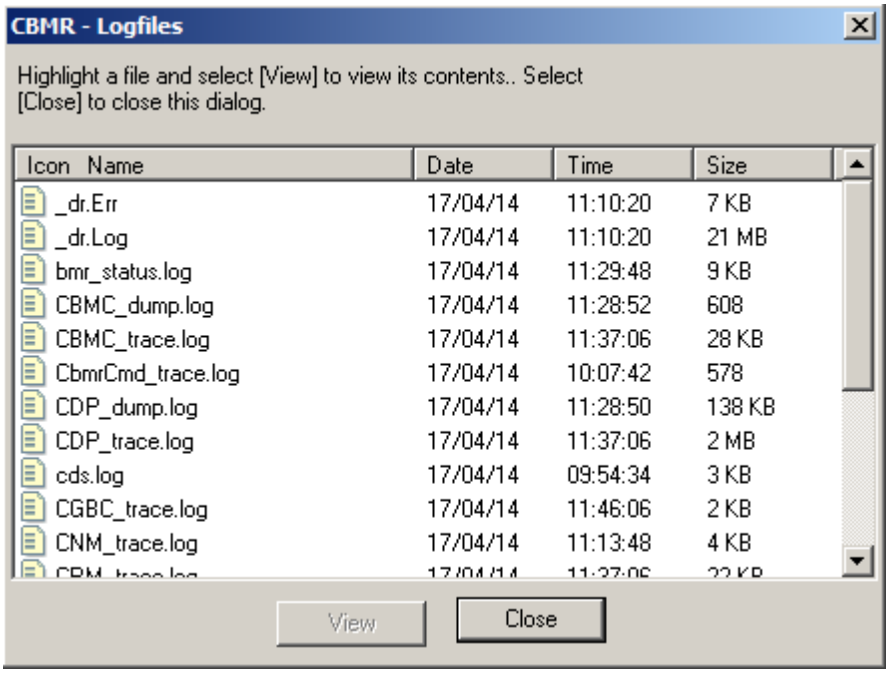

CBMR - Dynamic Driver Loading
Specify the location where the driver installation (.INF) file can be found .
Browse
Load
Cancel

The INF file and other associated driver files (such as the .SYS file) can be located on a CD, USB device or a network share. The following confirmation dialogue is displayed if the driver is loaded successfully:



3.4.2.5 Show Log and Error Reports

This main menu option allows the log files produced during the recovery to be viewed using Notepad. Normally, viewing this information is only required to diagnose a problem with the recovery.


CBMR - Logfiles
Highlight a file and select [View] to view its contents.. Select [Close] to close this dialog.
Icon Name
Date
Time
Size
_dr.Err 17/04/14 11:10:20 7 KB
_dr.Log 17/04/14 11:10:20 21 MB
bmr_status.log 17/04/14 11:29:48 9 KB
CBMC_dump.log 17/04/14 11:28:52 608
CBMC_trace.log 17/04/14 11:37:06 28 KB
CbmrCmd_trace.log 17/04/14 10:07:42 578
CDP_dump.log 17/04/14 11:28:50 138 KB
CDP_trace.log 17/04/14 11:37:06 2 MB
cds.log 17/04/14 09:54:34 3 KB
CGBC_trace.log 17/04/14 11:46:06 2 KB
CNM_trace.log 17/04/14 11:13:48 4 KB
View
Close

The important files are (this is not an exhaustive list):

bmr_status.log - restored disk and registry configuration log, eg. disks/partitions created summary

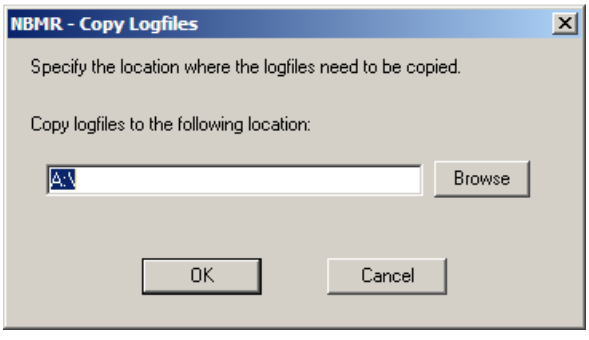
Copyright © 1998-2014 Cristie Software Ltd.

etc.
cbac_dump.log - contains a summary of the TSM client/server versions and node details.
cbac_trace.log - contains a detailed summary of the VTD access communications. Used by Cristie Support for diagnosing VTD problems.
cbmc_dump.log - contains a summary of the VTD details and datasets used in the recovery.
cbmc_trace.log - contains a detailed summary of the TSM client/server communications. Used by Cristie Support for diagnosing TSM access problem.
CbmrCmd_trace.log - contains CBMR product version information.
cdp_dump.log - contains general information regarding the system BIOS, disk configuration and timezone details of the original system.
cdp_trace.log - contains a detailed summary of how the partitions were restored. Used by Cristie Support for diagnosing disk configuration problems.
cds.log - Cristie deployment service log; used by Cristie Support to diagnose comms problems with other Cristie products, for example RecoverySimulator.
CGBC_trace.log - Cristie Generic Backup Client log file.
cnm_trace.log - contains network library information. Used by Cristie Support.
CRM_trace.log - contains the Recovery Manager log. Used by Cristie Support.
CRMWizard_trace.log - contains the clone settings used during the recovery. Used by Cristie Support.
dsierror.log - TSM interface log information
network.log - contains NIC hardware summary, current network configuration (eg. IP address, gateway IP address etc) and routing table.
RecoveryAgentService.log - Recovery Agent service log; used by Cristie Support to diagnose comms problems with other Cristie products, for example RecoverySimulator.
SEPInit_trace.log - Used to diagnose SEP Sesam recoveries.
setupapi.log - contains a summary of the Plug and Play devices detected by WinPE2 or WinPE4 as it boots. Used by Cristie Support for diagnosing WinPE2 or WinPE4 driver problems.
Version.log - Used by Cristie Support to determine version of Cristie CBMR software and DLLs deployed.

3.4.2.6 Copy Log and Error Report Files

Since all log and error files generated during the recovery are only transitory (ie. they are lost as soon as the Windows WinPE2 or WinPE4 environment exits), this option allows you to copy the files to a local device or remote network share for permanent record before booting the recovered system.

Use the **Cristie Network Configurator** utility to setup a network share first. All the files are compressed into a single ZIP file so that they can be easily sent to Cristie Support when required.



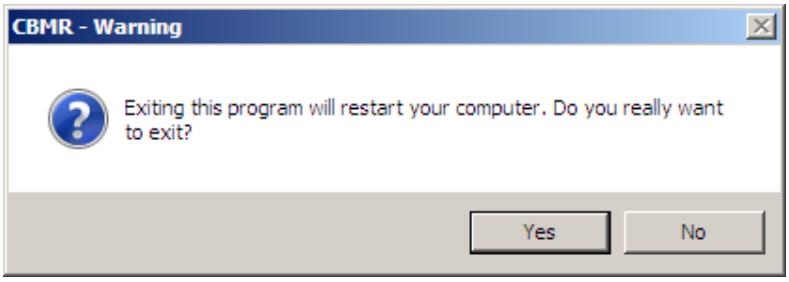
The example shows files being copied to a network share **A:**.

> ***Note: the logs are automatically written back to the recovered system after a successful recovery. They are saved to the CBMR installation sub-folder 'Temp'.***

3.4.2.7 Close Recovery Console and Reboot

After a successful recovery, select **Reboot** to exit the Windows WinPE2 or WinPE4 environment and boot the recovered system.

Press Yes on the confirmation warning to restart or No to continue running the DR console. If you choose to reboot, the recovered Windows system will boot into the OS:



Copyright © 1998-2014 Cristie Software Ltd.

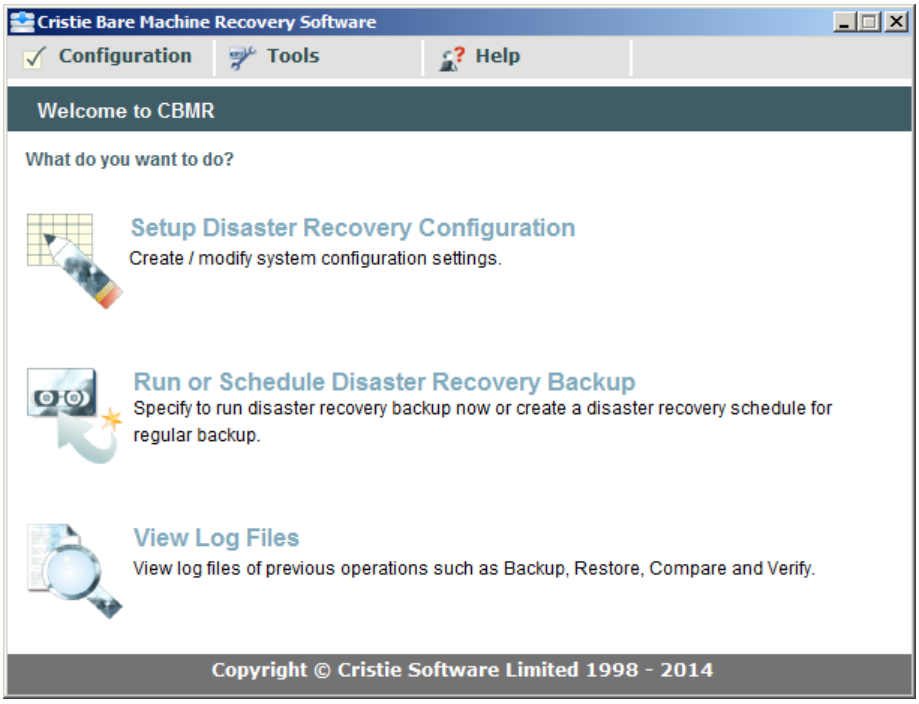
4 CBMR in More Detail

This section describes in full detail the many other features of CBMR. They enable it to be used as a conventional backup/restore product in addition to its primary function as a **Disaster Recovery** product.

4.1 User Interface Overview

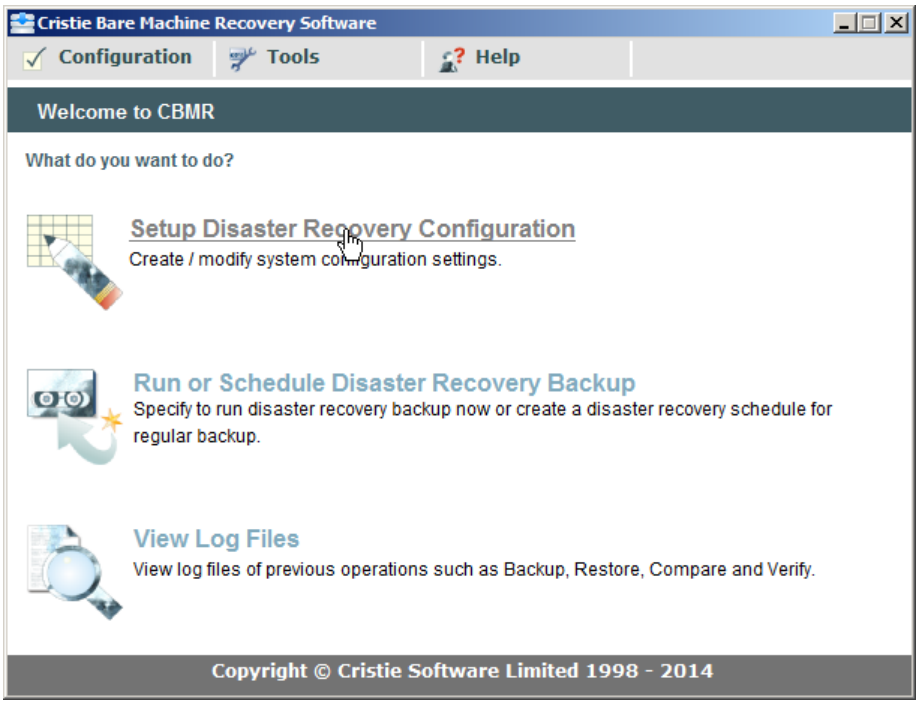
The CBMR main workspace is where most CBMR windows are opened. The main dialogue shows the most frequently used functions of CBMR. In addition, a menu bar runs along the top providing drop-down options for further features.

A Wizard is defined for each of the main tasks, such as setting up the system recovery information, creating or running a backup, managing backup locations, maintaining a catalogue of backups and defining the default options.


Cristie Bare Machine Recovery Software
Configuration
Tools
Help
Welcome to CBMR
What do you want to do?
Setup Disaster Recovery Configuration
Create / modify system configuration settings.
Run or Schedule Disaster Recovery Backup
Specify to run disaster recovery backup now or create a disaster recovery schedule for regular backup.
View Log Files
View log files of previous operations such as Backup, Restore, Compare and Verify.
Copyright © Cristie Software Limited 1998 - 2014

4.1.1 CBMR Setup Disaster Recovery Configuration

To invoke, click on **Setup Disaster Recovery Configuration** from the CBMR main window.

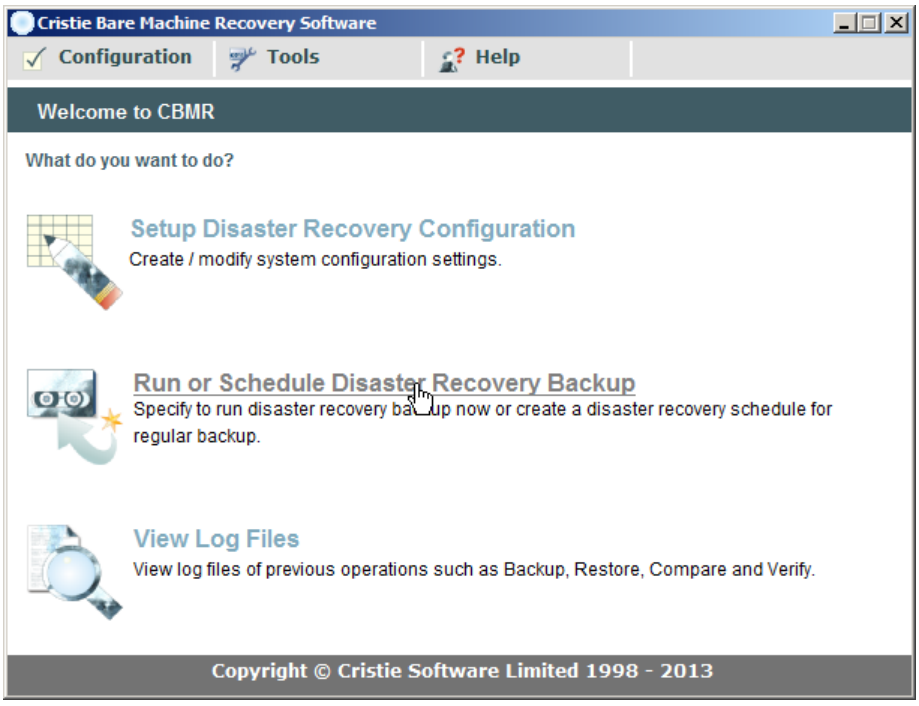

Cristie Bare Machine Recovery Software
Configuration
Tools
Help
Welcome to CBMR
What do you want to do?
Setup Disaster Recovery Configuration
Create / modify system configuration settings.
Run or Schedule Disaster Recovery Backup
Specify to run disaster recovery backup now or create a disaster recovery schedule for regular backup.
View Log Files
View log files of previous operations such as Backup, Restore, Compare and Verify.
Copyright © Cristie Software Limited 1998 - 2014

Selecting this option allows the system configuration to be created. Note that this is always stored with the Disaster Recovery backup itself.

For detailed instructions, please see the The Create Configuration Wizard chapter.

4.1.2 CBMR Run or Schedule Disaster Recovery Backup

To invoke, click on **Run or Schedule Disaster Recovery Backup** from the CBMR main window:


Cristie Bare Machine Recovery Software
Configuration
Tools
Help
Welcome to CBMR
What do you want to do?
Setup Disaster Recovery Configuration
Create / modify system configuration settings.
Run or Schedule Disaster Recovery Backup
Specify to run disaster recovery backup now or create a disaster recovery schedule for regular backup.
View Log Files
View log files of previous operations such as Backup, Restore, Compare and Verify.
Copyright © Cristie Software Limited 1998 - 2013

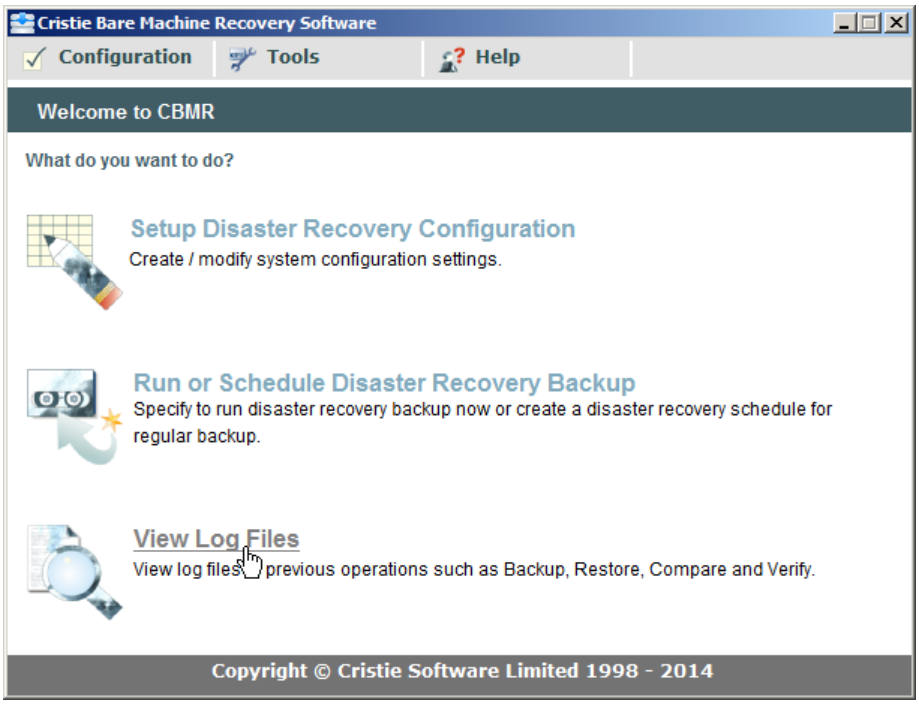
Copyright © 1998-2014 Cristie Software Ltd.

For more information, please see the Creating a Disaster Recovery Backup chapter.

4.1.3 View Log Files

When a backup or restore operation is performed, progress messages can be stored in a log file. The level of information stored and the name of the log file is set in Backup Selection script properties (for backups) and in the options dialogue (for Restore, Compare and Verify operations).

To view existing log files select **View Log Files** from the main CBMR menu:

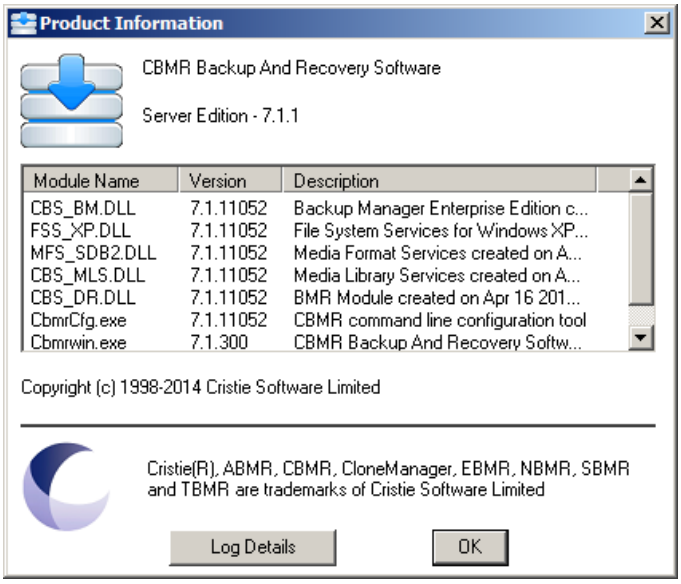

Cristie Bare Machine Recovery Software
Configuration
Tools
Help
Welcome to CBMR
What do you want to do?
Setup Disaster Recovery Configuration
Create / modify system configuration settings.
Run or Schedule Disaster Recovery Backup
Specify to run disaster recovery backup now or create a disaster recovery schedule for regular backup.
View Log Files
View log files previous operations such as Backup, Restore, Compare and Verify.
Copyright © Cristie Software Limited 1998 - 2014

If you request a log file to be created, the file is automatically saved and can be viewed using this option.

You can view or delete existing log files.

> *Note: there will be no log files present unless you have previously run a Backup, Restore, Compare or Verify which requests one to be created.*

Cristie's Support personnel may ask for a CBMR version log to help in diagnosing problems with your CBMR installation. This is a text file containing a list of components and their corresponding version numbers. To do this, select **Log Details** from the main **Help\About CBMR** menu option.


Product Information
CBMR Backup And Recovery Software
Server Edition - 7.1.1
Module Name Version Description
CBS_BM.DLL 7.1.11052 Backup Manager Enterprise Edition c...
FSS_XP.DLL 7.1.11052 File System Services for Windows XP...
MFS_SDB2.DLL 7.1.11052 Media Format Services created on A...
CBS_MLS.DLL 7.1.11052 Media Library Services created on A...
CBS_DR.DLL 7.1.11052 BMR Module created on Apr 16 201...
CbmrCfg.exe 7.1.11052 CBMR command line configuration tool
Cbmrwin.exe 7.1.300 CBMR Backup And Recovery Softw...
Copyright (c) 1998-2014 Cristie Software Limited
Cristie(R), ABMR, CBMR, CloneManager, EBMR, NBMR, SBMR and TBMR are trademarks of Cristie Software Limited
Log Details
OK

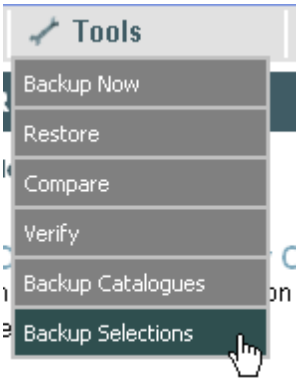
A file called version.log is created and can be viewed using the **View Log Files** option as before. See also the Show Log Report chapter in this document.

4.1.4 CBMR Tools

The CBMR Tools option presents the Backup Now, Restore, Compare, Verify, Backup Catalogues and Backup Selections functions. These are the main tasks that you will perform when maintaining your backup routines.

4.1.5 CBMR Backup Selection Tool

The **Backup Selection** tool contains scripts for performing regular backup jobs. To view the backup selections, click on the **Tools** drop-down menu and select Backup Selections.



All saved scripts are created by this tool.

A backup selection script defines the files and folders that will be backed up, along with various options such as the Backup Location on which the backup will be stored, the detail that will be saved in the backup catalogue, and the amount of information that will be stored in the backup catalogue. Essentially, a backup selection script defines the What and the How of a backup.

CBMR is supplied with a pre-defined script called system.scp. This script will backup all the files on Drive C: to the default backup location.

You can modify the system.scp script to suit your backup job, or you can use the options in

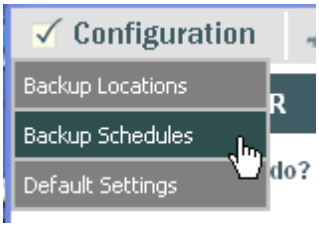
Copyright © 1998-2014 Cristie Software Ltd.

'Create New Backup Selections' to create your own scripts.

The CBMR Tools option presents the Backup Now, Restore, Compare, Verify, Backup Catalogues and Backup Selections functions. These are the main tasks that you will perform when maintaining your backup routines.

4.1.6 Backup Schedules

To invoke the **Backup Schedules** configuration tool, click on the **Configuration** drop-down menu and select Backup Schedules:



From here you can control existing scheduled jobs (Hold, Release, Run, Delete, Modify) or create new ones.

The Scheduler is a simple way of maintaining your Backup regime. Once you have created the backup selection scripts (what needs to be backed up and how) and created schedules for them, the scheduler will simply carry on and do the work without further intervention.

If Backup Scripts define the What and the How of a backup, then Schedules define the When.

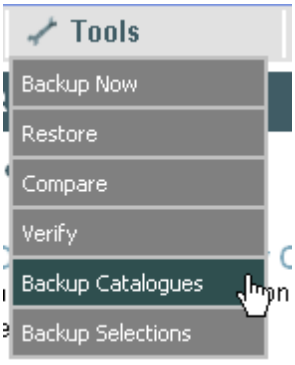
CBMR supports two services for running scheduled jobs: the **CBMR Scheduler Service** and the **Microsoft Windows Task Scheduler** service. Both provide the facility to schedule jobs for unattended running. The Microsoft Windows Task Scheduler service allows more flexible schedules to be configured, but the CBMR scheduler service is more tightly integrated into CBMR.

The Default Settings option can be used to configure whether the Scheduled Jobs tool displays jobs scheduled through the Windows Task Scheduler service or the CBMR Scheduler service.

See also the Scheduler Overview section of this document.

4.1.7 Backup Catalogue

The **Backup Catalogue** is a list of previous backups (backup volumes). To view the catalogue, click on the **Tools** drop-down menu and select Backup Catalogue:



Each time a backup is performed, a new Volume can be created in the Backup Catalogue. A

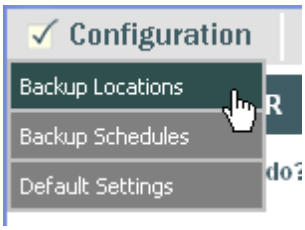
Backup Catalogue entry holds a list of the files and folders backed up. This catalogue can be browsed and queried, allowing you to find the location of backed up data without having to load tapes (if relevant).

The Backup Catalogue tool displays existing backups. You can view the catalogue entries, search for individual entries, create new ones or delete existing entries.

For more detailed information, see the Backup Catalogue section of this document.

4.1.8 Backup Locations

To invoke the **Backup Locations** configuration tool, click on the **Configuration** drop-down menu and select Backup Locations:



A Backup Location reprsents any physical device you use to backup your data. For example, a tape streamer, an autochanger or tape library, or a Virtual Tape Device, IBM Tivoli or Cristie Storage Manager device.

The **Backup Location Configuration** option holds details of all the Backup Locations currently configured within CBMR. Locations can be deleted, queried, backed up to and restored from using the Backup Location Tool. At least one Backup Location must be configured within CBMR.

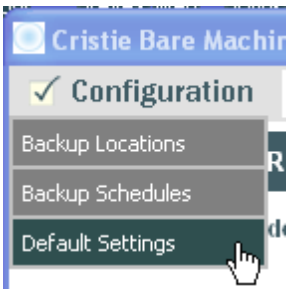
When CBMR first starts, no Backup Locations will be configured.

Backup, Restore, Compare, Verify and Media Utilities will all automatically use the default backup location unless otherwise directed.

Please see Configuring Backup Locations for further details.

4.1.9 CBMR Default settings window

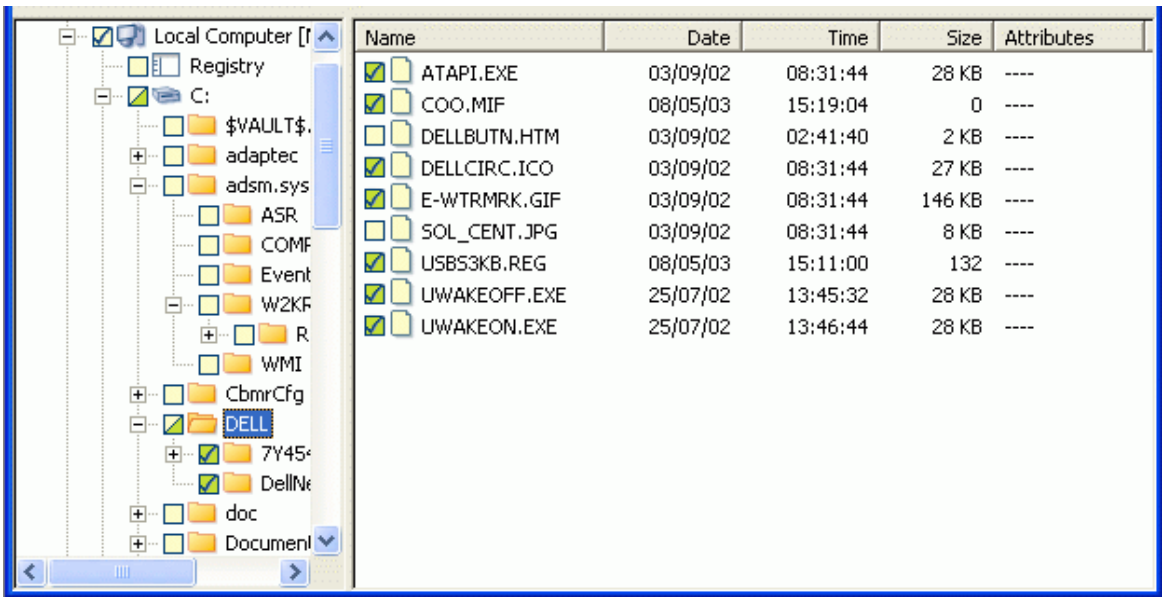
CBMRhas a range of defaults which can be adjusted with **Default Settings** configuration. These include a set of rules which direct CBMR during a backup. For example, what actions apply to a Backup (Append/Overwrite, compression on/off, Save Security Information and so on). To invoke this option, select the Default Settings option from the **Configuration** drop-down menu:



This takes you directly to the Default Settings property sheet. Default settings relating to backup are used by all backups unless you specify otherwise in the individual backup location script's properties.

Copyright © 1998-2014 Cristie Software Ltd.

4.1.10 Directory Tree



Several screens in CBMR present a two-pane explorer-style view containing a directory tree on the left and a file list on the right. These windows enable you to select items to be backed up, restored, verified or compared.

The Directory Tree pane displays the directory structure of the selected resource, be it your computer's drives and folders when selecting items to be backed up, or the datasets and folders in a volume in the Backup Catalogue or tape within a Backup Location when selecting data to be restored, compared or verified.

The File List pane displays the files stored in the highlighted location in the Directory Tree pane.

To select (tag) or deselect (untag) an item in either the tree or list pane, click on the square box next to the item's icon. Items can also be tagged and untagged by highlighting them and selecting Tag/ Untag from the Item menu or the context menu.

If you know that you are going to tag most of the drive or dataset contents except for one or two directories or files from within, then tag the drive or dataset first and untag the directory or files as required. If on the other hand you want to exclude more than you include, then start with the drive or dataset untagged and tag the directories and/or files individually from this window.

When an item in the file list pane is highlighted, the list can be sorted in a number of ways using the **Sort** menu. The file list can also be sorted by clicking on the list's column headers.

+ A plus sign in the tree pane indicates that the tree item can be expanded. Expand it by clicking on the plus sign.

- A minus sign in the tree pane indicates that the tree item has been expanded to its lower level. It can be contracted by clicking on the minus sign.

The status of an item is indicated by the square box next to it. Items can be tagged or untagged by clicking on this box. Listed below are the various symbols the status box can show.

All tagged.

Partial tagging. At least one directory or file has been untagged.

Nothing tagged.

A restriction has been applied to this selection.

Item that cannot be directly tagged, though you may open it and tag or untag its contents.

At least **one item** is tagged for backup; it does **NOT** mean that every item underneath is tagged.

4.2 Getting Started

CBMR allows you to backup any data on your system to any Backup Location (excluding DVD/CD-writers) attached to your computer or network. You can then examine the content of the backup and restore any desired files/directories.

To use CBMR you must:

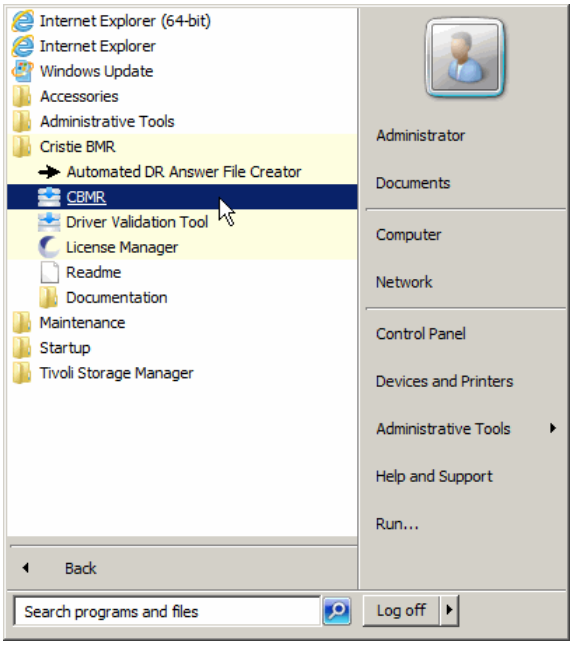
1. Install the CBMR software
2. Set up the Backup Location storage device(s)
3. Set up Backup Selection scripts to do appropriate backups
   - if you wish, you can also set up the Scheduler to perform backups

You can then

- Perform a regular cycle of backups using the Scheduler
- Find data that you have backed up using the Backup Catalogue Utility
- Restore data from backups

When the software is successfully installed, CBMR is available from the **Programs** menu in the **Start** popup. The example below shows CBMR about to be started:

Copyright © 1998-2014 Cristie Software Ltd.



A shortcut

to CBMR is also created on the desktop during installation .CBMR may also be started by clicking on this shortcut.

4.2.1 Configuring CBMR

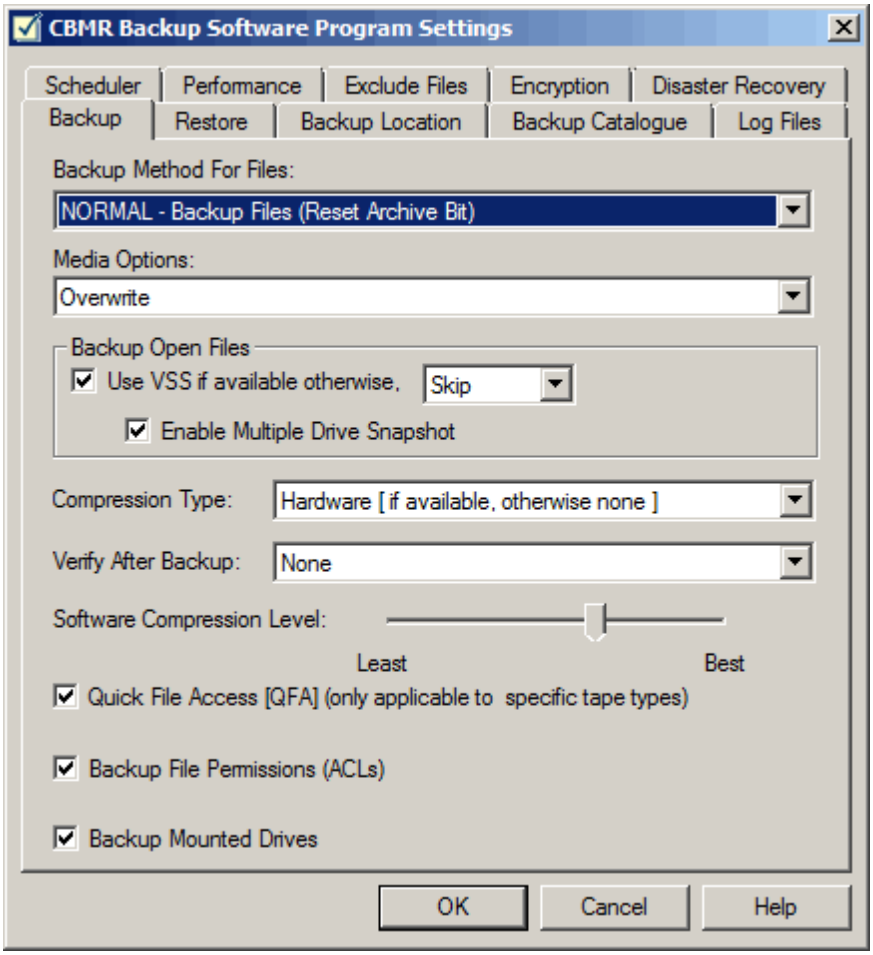
CBMR is supplied ready to use, with program settings already defined. However, you should check the program defaults to ensure that they are appropriate to your Disaster Recovery or Backup and Restore requirements.

All the information is contained in property pages. Each page is dedicated to a different section of the configuration, making it easy to locate a particular area if you need to make changes.

The default program settings, once defined, will generally remain unchanged. If you want to apply different rules for a particular job, then you can modify the settings from within the **Backup Selection** script and these will apply only to the current script.

4.2.1.1 Default Settings

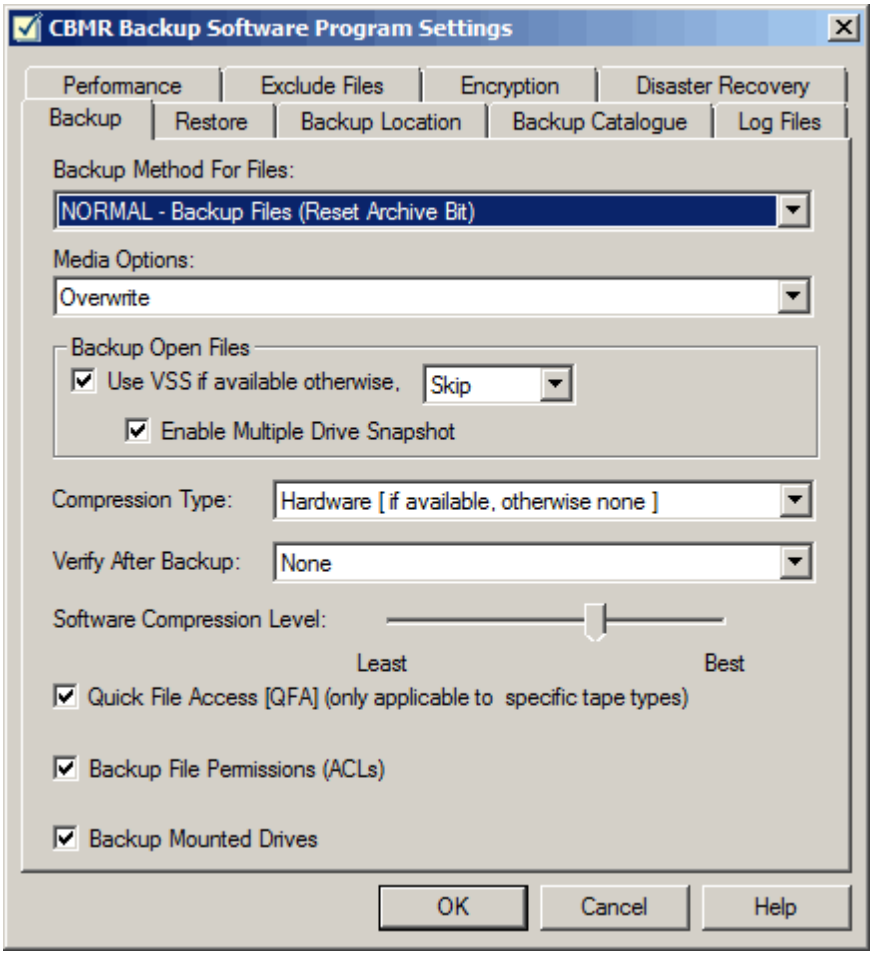
To invoke the **Default Settings** configuration, select it from the **Configuration** toolbar. If the Default Settings configuration is invoked from a Wizard or other tool, CBMR opens the relevant page. For example, if you are in the **Backup Catalogue**, the Backup Catalogue tab is displayed; if you are in **Backup Location**, the Backup Location tab is displayed.



Copyright © 1998-2014 Cristie Software Ltd.

Backup Properties

This page allows you to set the default actions which will apply during a backup. The defaults can be over-ridden in the properties for individual backup selection scripts.



Backup Method For Files

There are four pre-configured backup methods to choose from.

NORMAL - Backup Files (Reset Archive Bit)

The Normal selection will backup all the selected files and reset the archive bit

COPY - Backup Files

The Copy selection will backup all the selected files without affecting the archive bit

DIFFERENTIAL - Backup Changed Files

The Differential selection will backup all files that have changed or are new since the last Normal or Incremental backup. The backup will not affect the archive bit

INCREMENTAL - Backup Changed Files (Reset Archive Bit)

The Incremental selection will backup all files that have changed or are new since the last Normal or Incremental backup. The backup will reset the archive bit

Media Options

The media options control the way that data is written to the media.

Overwrite - If overwrite is selected the backup will start at the beginning of the media overwriting

any existing data

Overwrite media with the same label, append otherwise - Selects overwrite only if the media label matches with the requested media, otherwise the data will be appended to the media

Overwrite media with the same label, fail otherwise - Selects overwrite only if the media label matches with the requested media, otherwise the operation fails and no data will be written to the media

Append, overwrite if not appendable - Selects append, but if the media is blank or the media contains a non CBMR data set and therefore cannot be appended, the media is overwritten

Append to media with the same label, fail otherwise - Selects append only if the media label matches with the requested media, otherwise the operation fails and no data will be written to the media

Backup Open Files

When selecting the Backup Open Files option, CBMR will use Microsoft VSS if installed and running, while backing up open files. If VSS is not installed or the option is not selected, then the option to **Automatically** retry the open file, **Skip** the open file or **Ask** the user what to do can be selected from the list box. If VSS is in use, then a further option is available to enable multiple-drive monitoring.

Compression Type

The type of data compression can be selected to be:

None - Data is not compressed

Software Data compression will be performed by the CBMR software before the data is written to the Backup Location

Hardware compression (if available, otherwise none) This option will attempt to make the Backup Location perform the data compression. If compression is not available on the hardware, the data will remain uncompressed

Hardware compression (if available, otherwise Software) By preference, data compression will be performed by the hardware if it is possible, otherwise compression will be done by CBMR software

Software Compression Level A slider control is provided to set the software backup compression level. It can be set from level 1 (least compression) up to level 9 (best compression), level 6 being the default. Note that minimum (least) compression provides maximum backup performance. Also note that increasing the compression level will extend the backup time. This setting only applies when the *Software Compression* type is selected for a backup

Verify After Backup Checks the validity of the recorded media

None Does not perform any checks

Check Integrity alone After finishing the backup, the media will be scanned from the beginning to end, ensuring it is readable

Byte By Byte comparison After finishing the backup, each file on the media will be compared against its disk counterpart and the differences reported

Quick File Access (QFA)
This option, if ticked will provide rapid access to files during a restore operation. (Not all drives support this option)

Copyright © 1998-2014 Cristie Software Ltd.

Save File Permissions (ACLs)

Select this option (ticked) if you want the security information (access control data) associated with directories and files as well as the data included in the backup. If the option is not ticked then only the data is included.

The user who is logged on must have the appropriate '*Right*' to request security information to be backed up. Please check with your System Administrator that your user account has been included in the Backup Operators group.

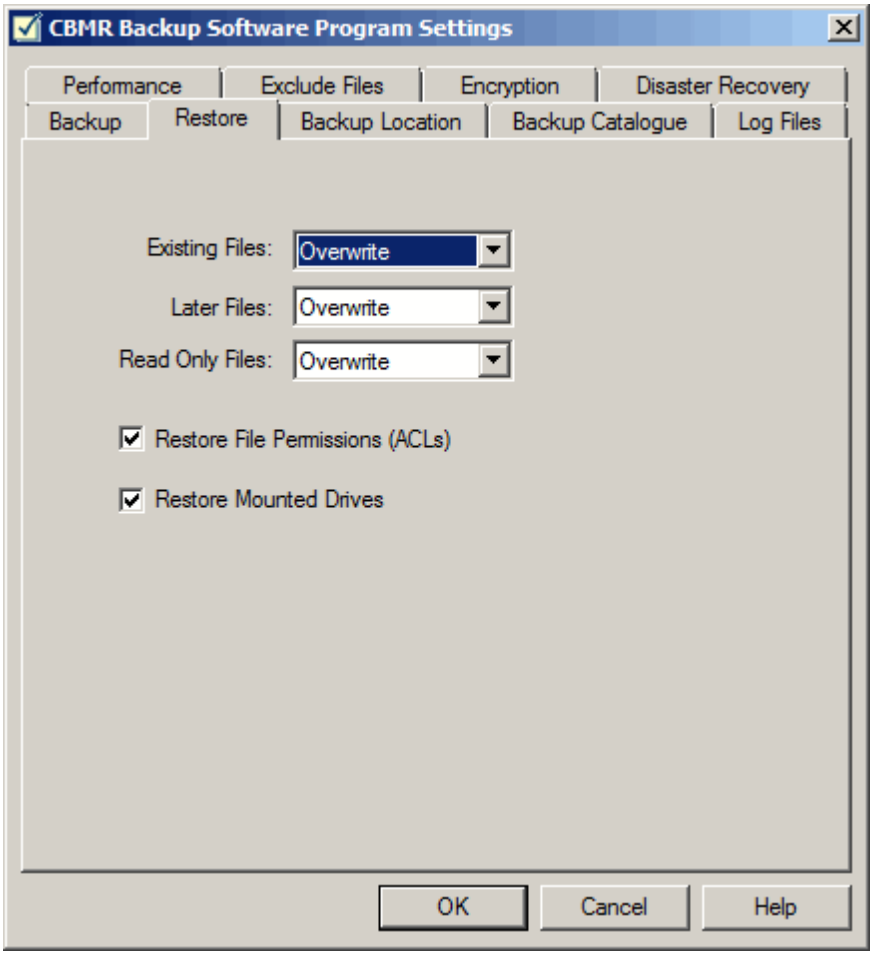
If this option is enabled then all the security details (access control data) are included in the backup as well as the data.

Backup Mounted Drives

By default all mounted drives (ie. partitions) will be included in the backup. Deselect this option so that mounted drives are excluded from the backup by default.

Restore Properties

This page allows you to set the default actions which will apply during a Restore job. The defaults can be over-ridden when performing individual restores.



Existing Files

If any files being restored already exist on disk, then you can direct CBMR to respond in one of the following ways:

Skip any file it encounters which already exists.

Ask whether it should overwrite or skip the file.

Overwrite the existing file with the file from the backup.

Later Files

If any files being restored are found to be later versions than those already existing on disk then you can direct CBMR to respond in one of the following ways:

Skip any file it encounters which are later versions.

Ask whether it should overwrite or skip the file.

Overwrite the file on disk with the later version from the backup.

Read Only Files

If any read only files being restored already exist on disk then you can direct CBMR to respond in one of the following ways:

Skip any read only file it encounters which already exists on disk.

Ask whether it should overwrite or skip the file.

Overwrite the file on disk with the file from the backup.

Restore File Permissions (ACLs)

If this option is selected CBMR will restore the Access Control List information associated with directory files included in the restore. If the option is not ticked then only the data is restored.

Restore Mounted Drives

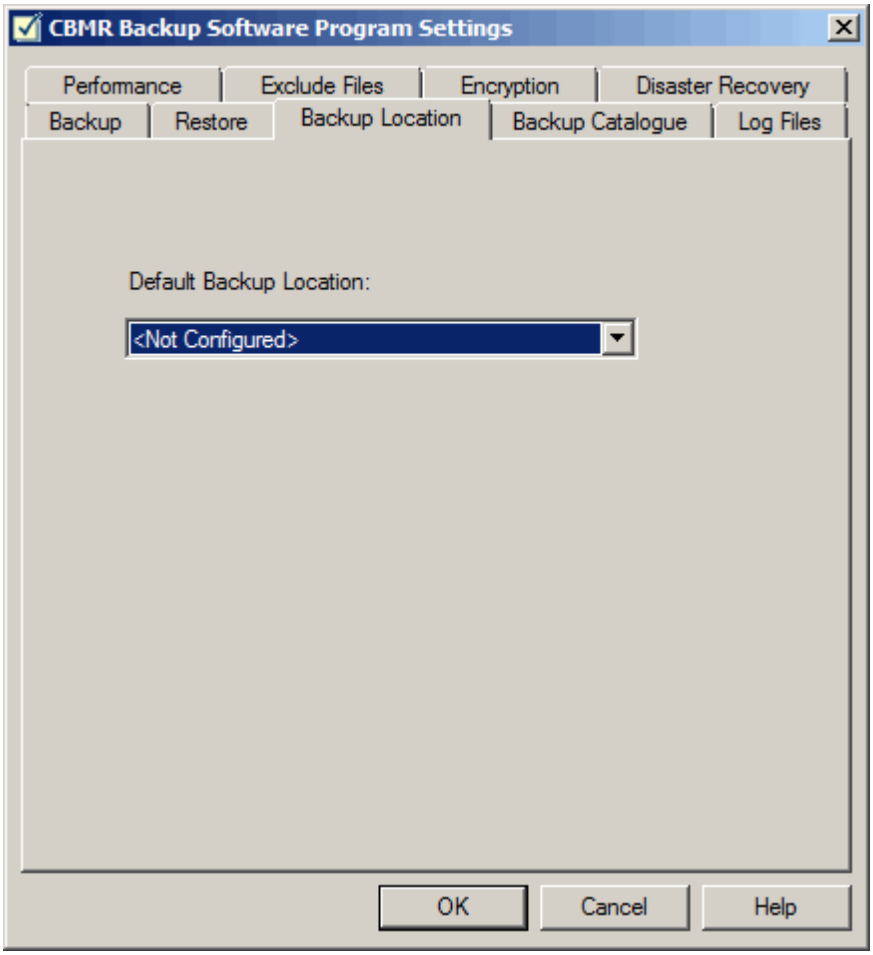
If this option is selected any mounted drives (partitions) will be restored as well.

Note: you must be logged on the computer as a user account with the appropriate rights to restore security data.

Backup Location Properties

This page allows you to select a default backup location for all future Backup, Restore, Compare and Verify operations. The selection will show all configured **Backup Locations**. CBMR will always use the default location for Backup, Restore, Compare and Verify jobs initiated from the Executive window.

Copyright © 1998-2014 Cristie Software Ltd.



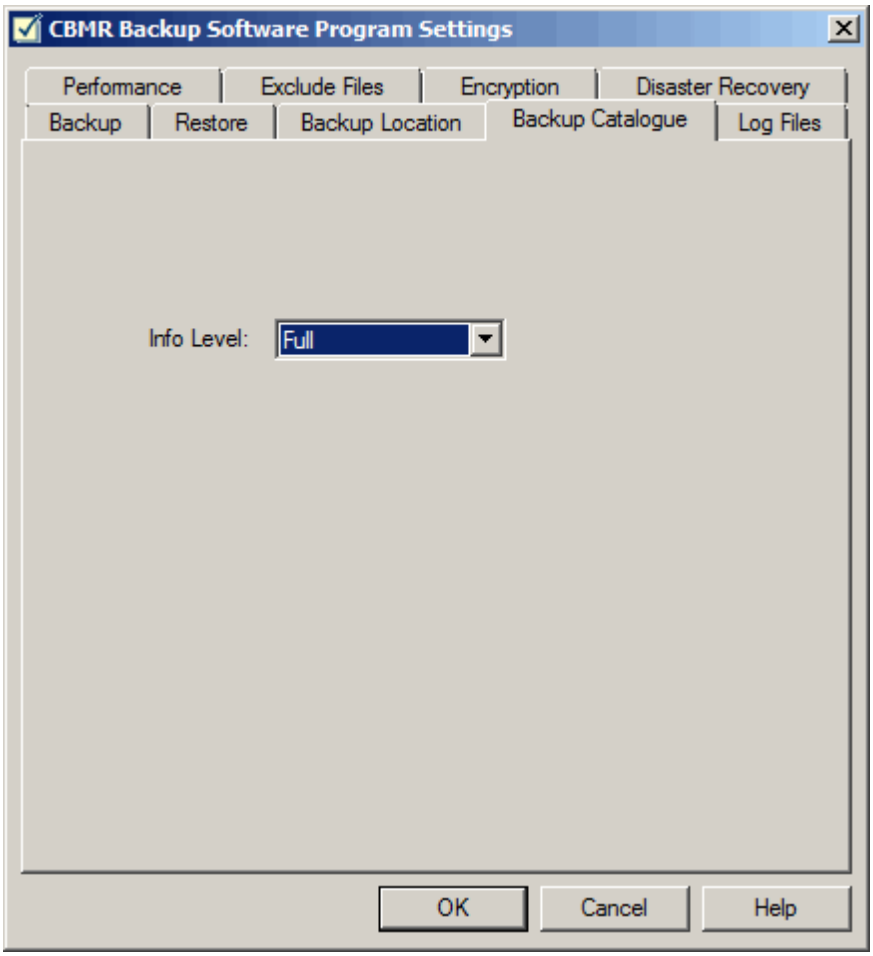
If you need a location which does not appear in the list, then you need configure it using **Create New Backup Location** in the Backup Locations folder.

> ***Note: if necessary, you can assign a different Backup Location from within the Backup Selections script to be used for a particular job. This does not affect the default.***

Restore, Compare and Verify jobs can be run on a non-default location by selecting another backup location in the **Backup Location** dialogue and selecting **Restore / Compare / Verify...** from its context menu.

Backup Catalogue Properties

This page allows you to define the level of information which is recorded in the **Backup Catalogue** when a backup is run.



There are four different levels:

Full - Media and Dataset headers, Directories plus File information. (This level of detail will use a significant amount of disk space)

Partial - Media and Dataset headers plus Directories

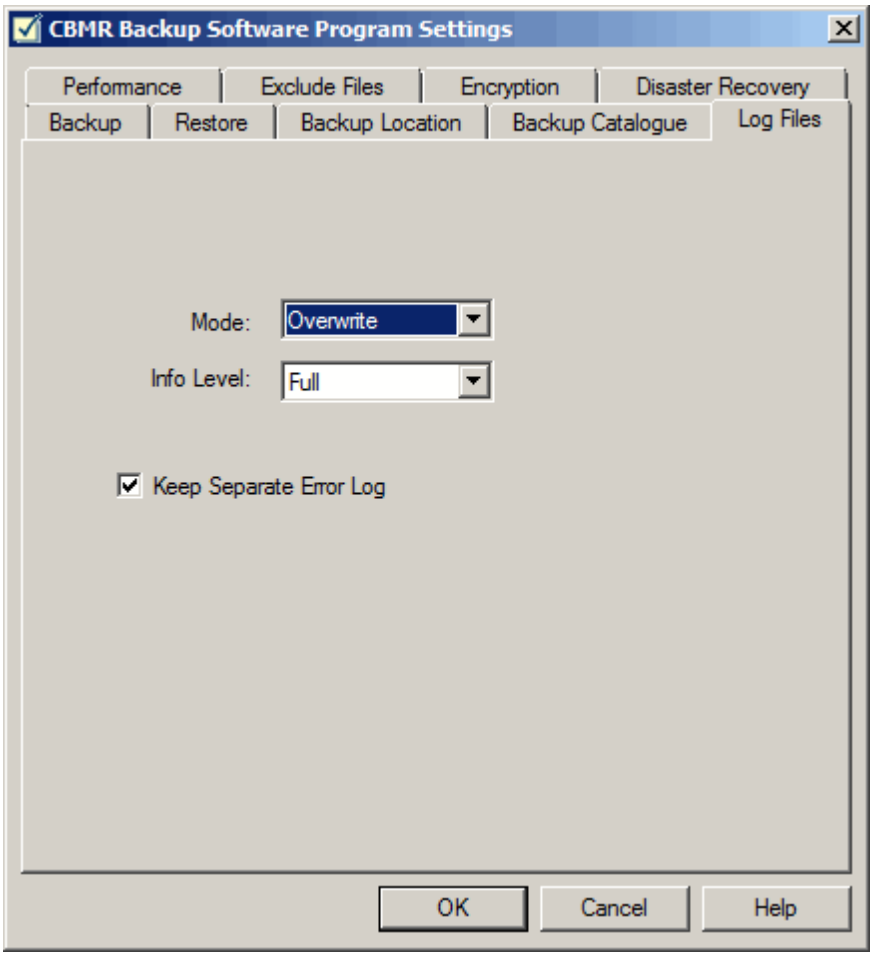
Brief - Media and Dataset headers only

None - No details of the backup are recorded in the Backup Catalogue

Copyright © 1998-2014 Cristie Software Ltd.

Log File Properties

Log files are a useful source of information and will list any error messages. Log file information can be important if problems have occurred.



The following options are available:

Mode - Overwrite/Append

If **Overwrite** is set, then each time the log file is created it overwrites the existing one

If **Append** is set, then each log file is appended to the previous one

Info Level - Full/Partial/Brief/None

A **Full** logfile contains a list of all files, errors (if any) and statistics

A **Partial** log file contains sub-directories, errors (if any) and statistics

A **Brief** log file contains errors (if any) and statistics

If **None** is selected, then no log file is created

Keep Separate Error Log

If this option is ticked, an additional log file is created which lists errors only. Similar to the other log files, it takes the name of the current operation but with an extension of **.err** eg. **backup.err**

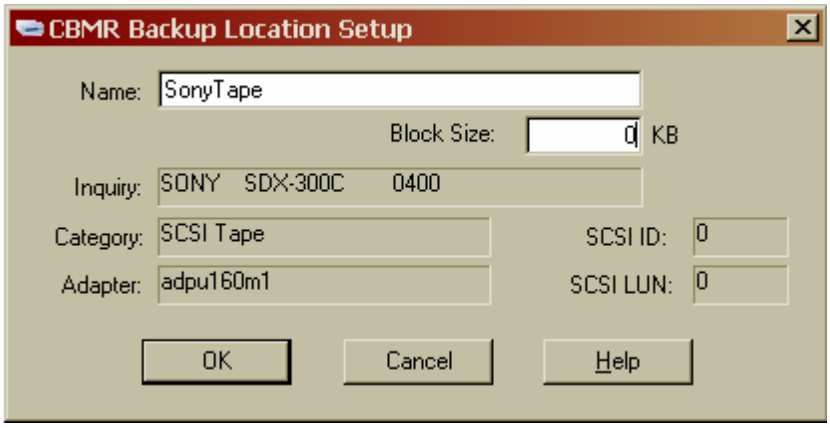
Errors will still be written to the Full, Partial or Brief log file if you have requested one of these.

Performance Page

CBMR has control over some performance related parameters, like the number and size of read/write buffers. The basic unit of data which can be read or written to the tape, called a block, is determined by CBMR, depending on the **Backup Location** device and media type in use. Most recent tape drive manufacturers recommend bigger block sizes for better performance. As a result, in CBMR version 4 the following configurable parameters were introduced.

Tape Block Size

It is possible to set individual block sizes for each Backup Location used by CBMR. This could be done using the Backup Locations dialogue:



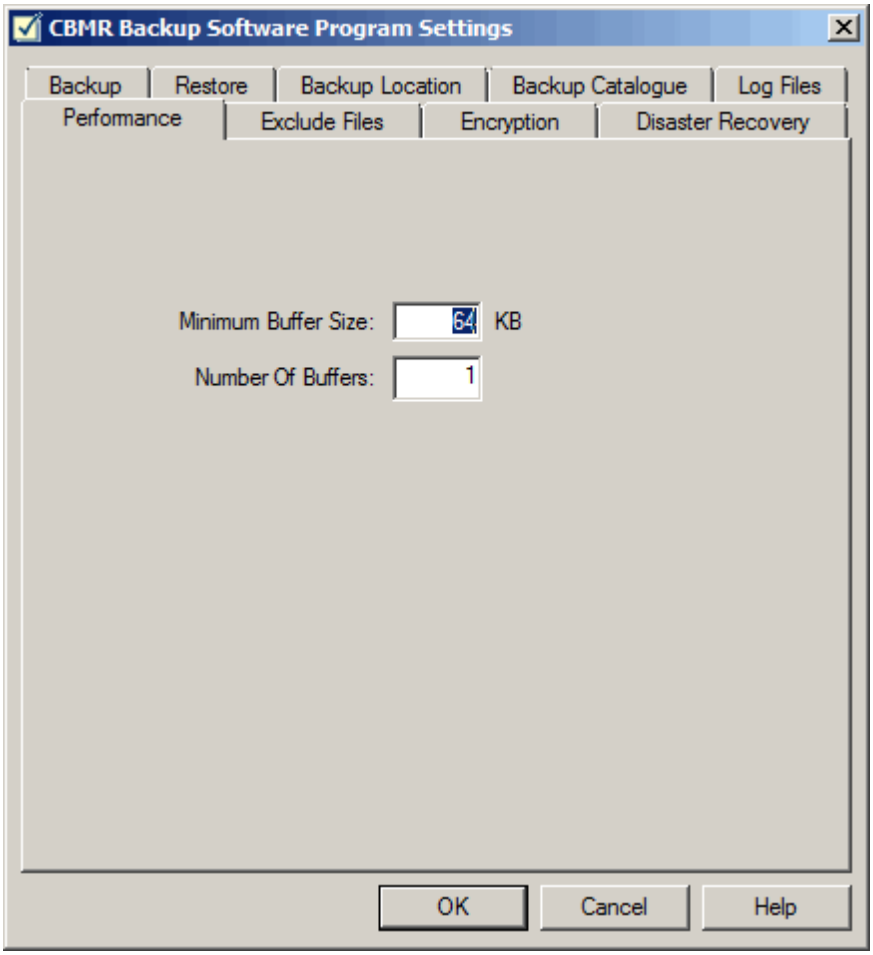
Minimum Buffer Size

The minimum buffer size can be set using the **Default Settings** property sheet, **Performance** page. This only sets the minimum buffer size. It is guaranteed that a buffer size over this limit will be used. The buffer size should be in multiples of the tape block size in use. Since it is possible to set block sizes individually for locations, CBMR will calculate the next integral multiple block size over this limit.

Number of Buffers

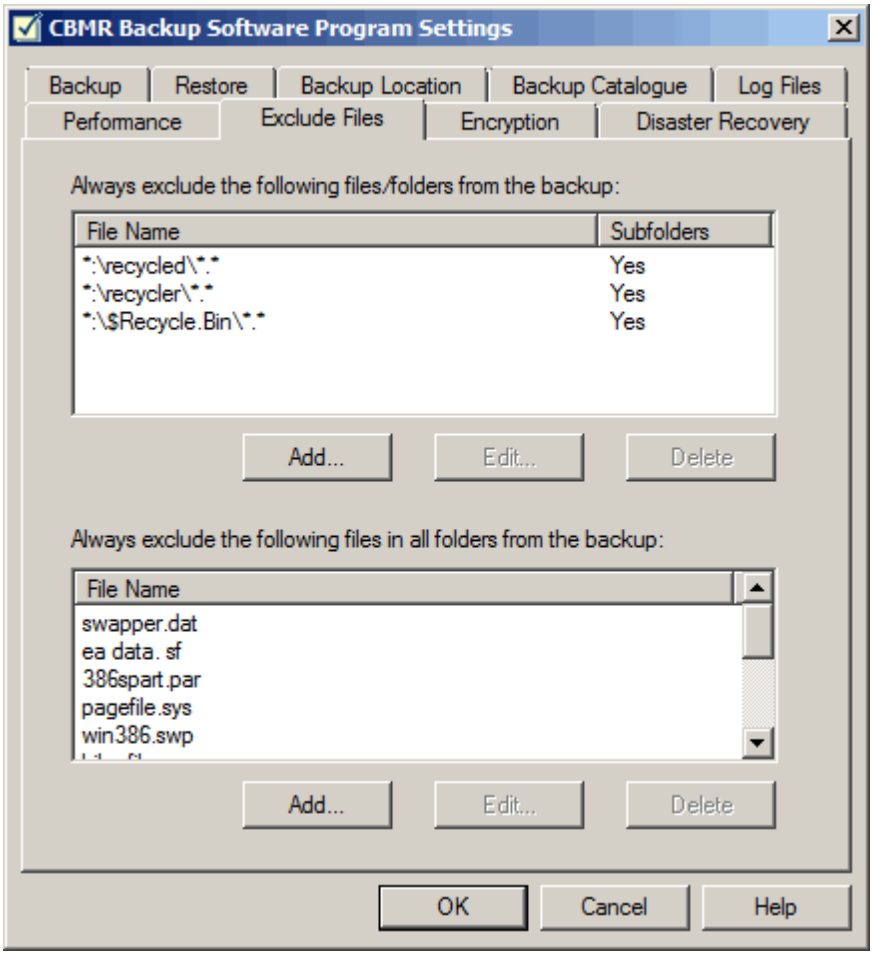
At least one buffer is required for any read/write operation. Increasing the number of buffers will increase the performance of the locations with high latency. This depends on the system configuration, location in use and the load on the system at the time of the backup. It is recommended to test with different values on a test backup.

Copyright © 1998-2014 Cristie Software Ltd.


CBMR Backup Software Program Settings
Backup
Restore
Backup Location
Backup Catalogue
Log Files
Performance
Exclude Files
Encryption
Disaster Recovery
Minimum Buffer Size:
64
KB
Number Of Buffers:
1
OK
Cancel
Help

Exclude Files

Allows selected groups of files or folders to be excluded from *all* backups.



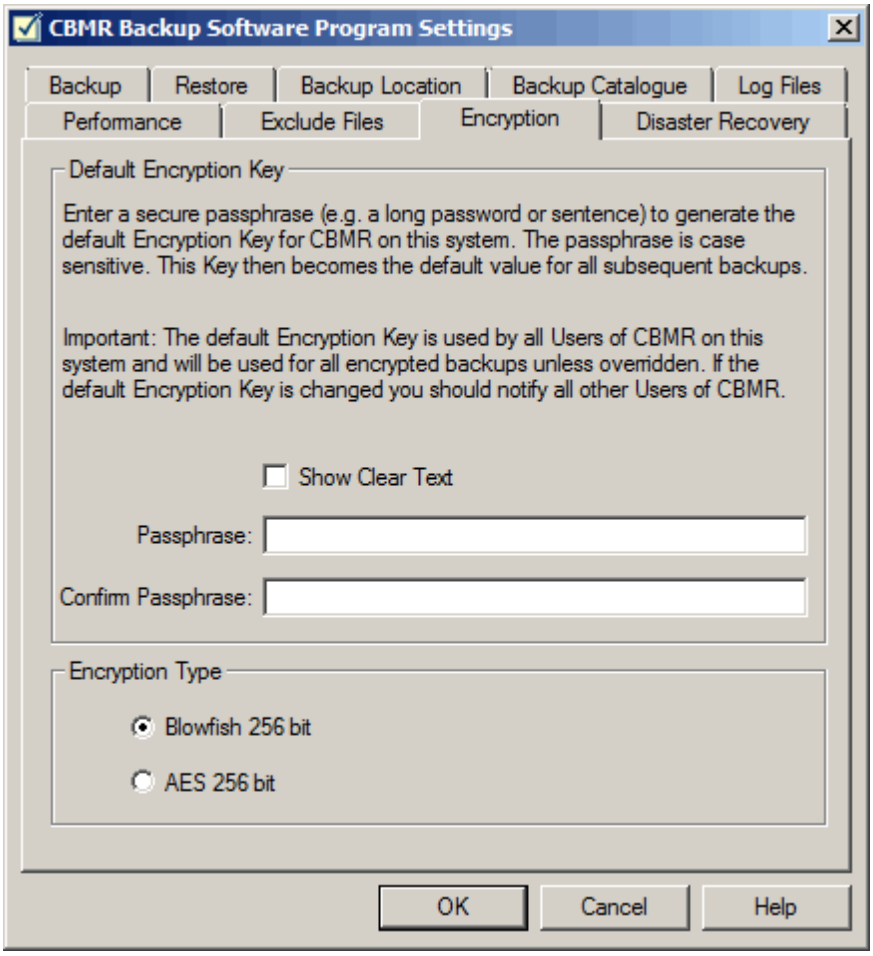
The upper section allows files and folders to be excluded from a backup using the wildcard characters * or ?. The wildcard characters are accepted for drive and filename, but not for the path. For example, ***:*.avi** will exclude all files with the extension **AVI** from a backup.

The lower section allows specific named files to be excluded from a backup. Note all files with the specified name regardless, on which drive or in which folder they reside, will be excluded from the backup. Wildcards are not accepted in this case.

Copyright © 1998-2014 Cristie Software Ltd.

Encryption Properties

This property page allows a default **passphrase** to be setup for encrypted backups.


CBMR Backup Software Program Settings
Backup
Restore
Backup Location
Backup Catalogue
Log Files
Performance
Exclude Files
Encryption
Disaster Recovery
Default Encryption Key
Enter a secure passphrase (e.g. a long password or sentence) to generate the default Encryption Key for CBMR on this system. The passphrase is case sensitive. This Key then becomes the default value for all subsequent backups.
Important: The default Encryption Key is used by all Users of CBMR on this system and will be used for all encrypted backups unless overridden. If the default Encryption Key is changed you should notify all other Users of CBMR.
Show Clear Text
Passphrase:
Confirm Passphrase:
Encryption Type
Blowfish 256 bit
AES 256 bit
OK
Cancel
Help

The passphrase is used internally by CBMR to generate an **Encryption Key**. The resulting Encryption Key then becomes the default value for all subsequent encrypted backups for all Users of CBMR on the system (unless overridden in a backup script). If this default is changed it is important to notify all other users that it has been changed.

If **Show Clear Text** is selected then the passphrase is shown in plain view, otherwise it is shown as asterisks as it is typed in.

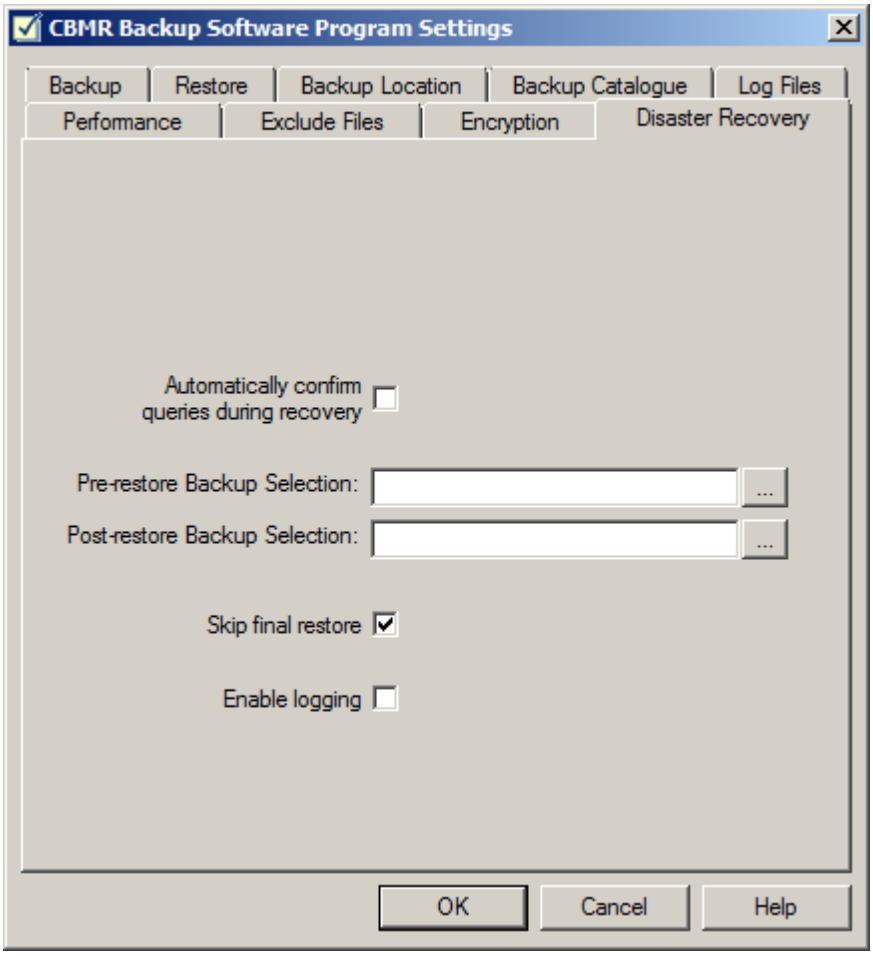
The passphrase should be secure (eg. a long sentence or password). Note the passphrase is case sensitive.

Two encryption algorithms are available - **Blowfish 256-bit** and **AES 256-bit**. Blowfish is generally faster to encrypt than AES. However, enabling encryption significantly slows down the backup.

Please refer to Backup Encryption for more details.

Disaster Recovery Properties Page

This page allows various default settings for Disaster Recovery to be configured.



Automatically confirm queries during recovery

During the disaster recovery process, the system will prompt for confirmation to perform some actions. If you would like the Disaster Recovery module to confirm these prompts for you, check this box.

Pre-restore script / Post-restore script

There may be a requirement to run custom commands before or after a disaster recovery restore operation. These commands should be entered into a windows '.cmd' file which can be linked to using these settings.

Skip final restore

If the final, post-recovery, restore should not be automatically run, select this option. The final restore can be manually run using the DR scripts.

Enable logging

This option configures the disaster recovery restore process to log status messages.

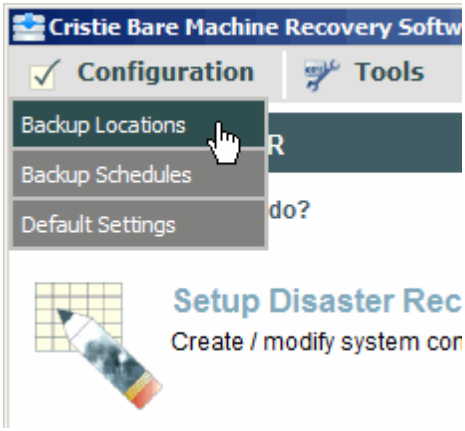
Copyright © 1998-2014 Cristie Software Ltd.

4.2.2 Configuring Backup Locations

To use a **Backup Location** within CBMR, you must first configure it. The configuration process allows you to give a custom name to your location, as CBMR is capable of finding all the directly attached locations automatically (not ITSM however).

CBMR must have at least one location configured in order to operate and backup data.

Configured locations are listed in the Backup Locations option selected from the **Configuration** toolbar:

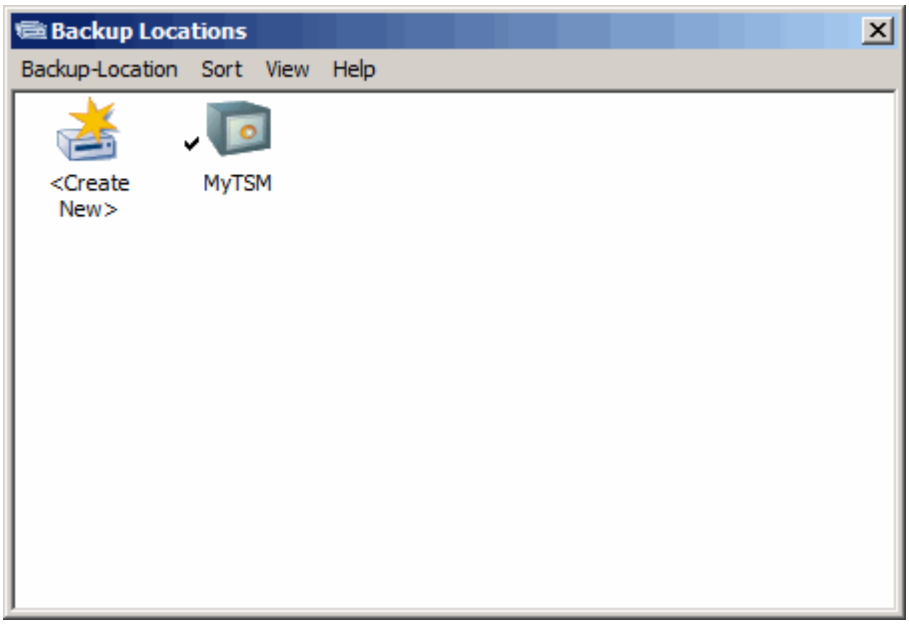


CBMR can use a variety of different backup locations.

These include:

- SCSI tape drives like DAT, DLT and SLR
- IDE tape drives like TRAVAN drives
- File locations like removable optical disks or files on a networked disk-drive
- All of the above locations cascaded to operate in sequence avoiding media change requests
- Library/Auto-Changers configured from Tape drives and Robotics/Media Handler mechanisms
- IBM TSM Server (with the Cristie TSM Client Module)

All the configured backup locations in CBMR are listed in the **Backup Locations** configuration. This is a one stop solution to create, modify and delete Backup Locations.



The Locations top bar menu contains options to:

- View the **Settings...** for the selected location

- Run a **Backup, Restore, Compare** or **Verify** on the selected location

- **Delete** the location

- Run Media Utilities

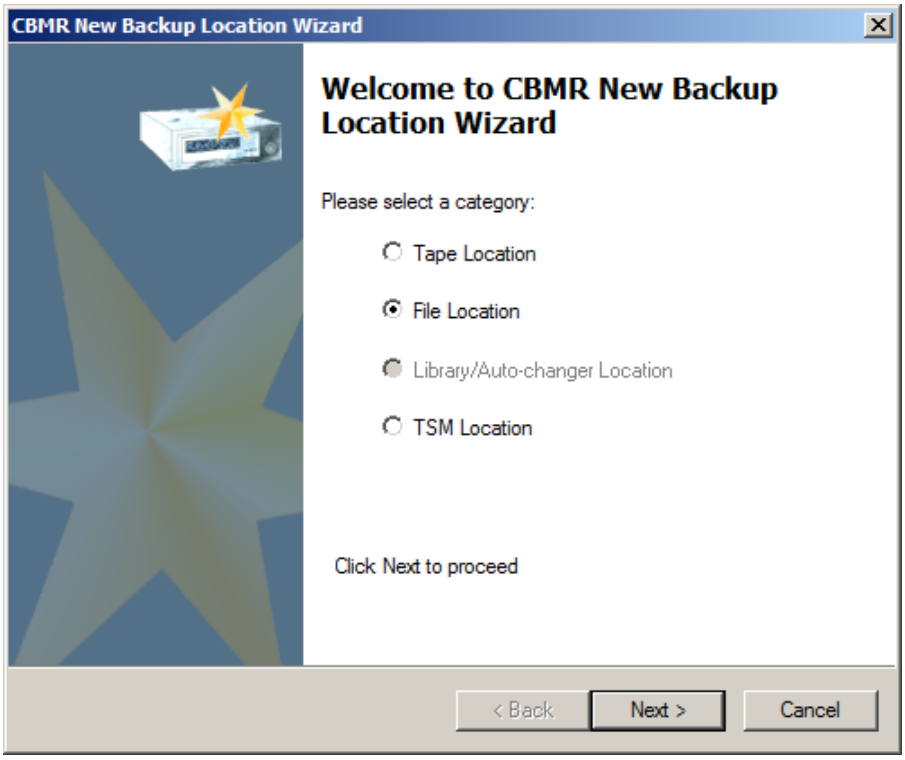
- Set the location to be the default location when running a Backup/Restore etc. (**Set as Default Location**)

The **Sort** top bar menu allows you to arrange the backup locations in alphabetic sequence (**Sort by Name**) or in date created sequence (**Sort by Category**).

> ***Note: if the Details view is displayed, you can also sort the entries by clicking the relevant column heading.***

4.2.2.1 New Backup Location

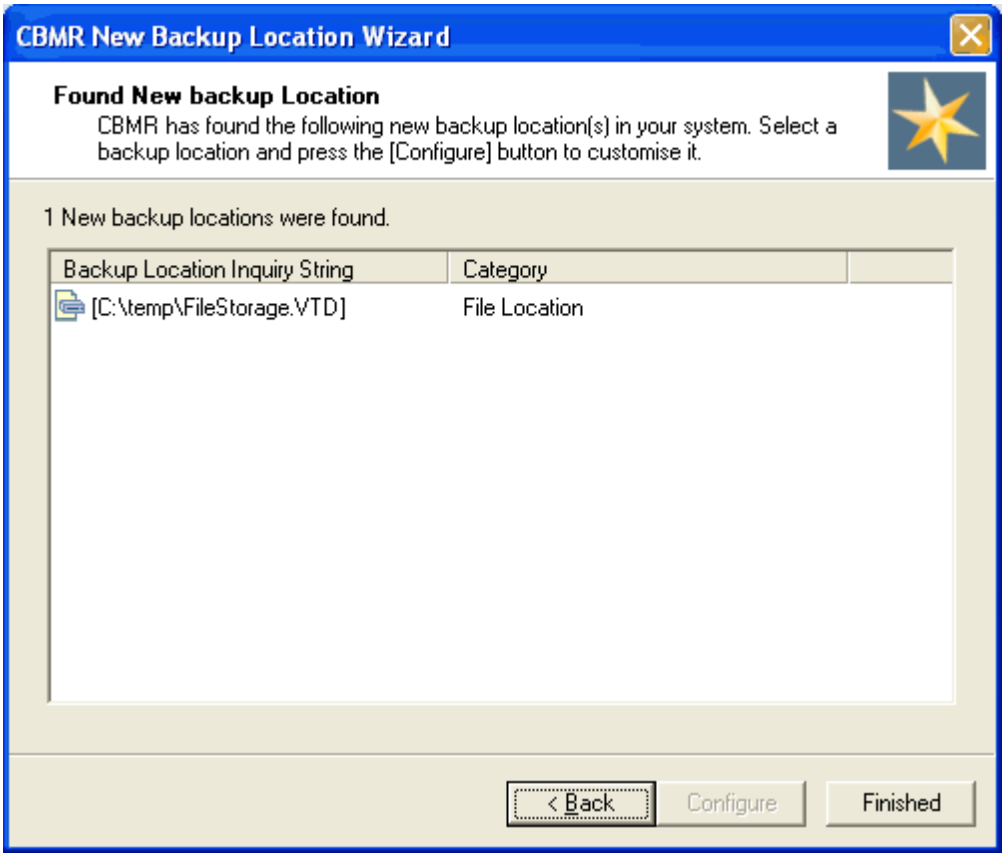
Selecting the **New** menu option or double clicking the **Create New** icon will invoke the **New Backup Location** Wizard. The Wizard allows you to configure various types of backup location.



If you let the CBMR Wizard **search automatically**, the **New Backup Location** Wizard will list the location devices that are directly attached to the system but are yet to be configured.

It displays the Inquiry string of each location - which is read from the device firmware and also the category of the backup location.

Copyright © 1998-2014 Cristie Software Ltd.


CBMR New Backup Location Wizard
Found New backup Location
CBMR has found the following new backup location(s) in your system. Select a backup location and press the [Configure] button to customise it.
1 New backup locations were found.
Backup Location Inquiry String
Category
[C:\temp\FileStorage.VTD]
File Location
< Back
Configure
Finished

The categories can be:

- SCSI tape

- Media Handler/Robotics (needs additional library support module from Cristie)

- File Device

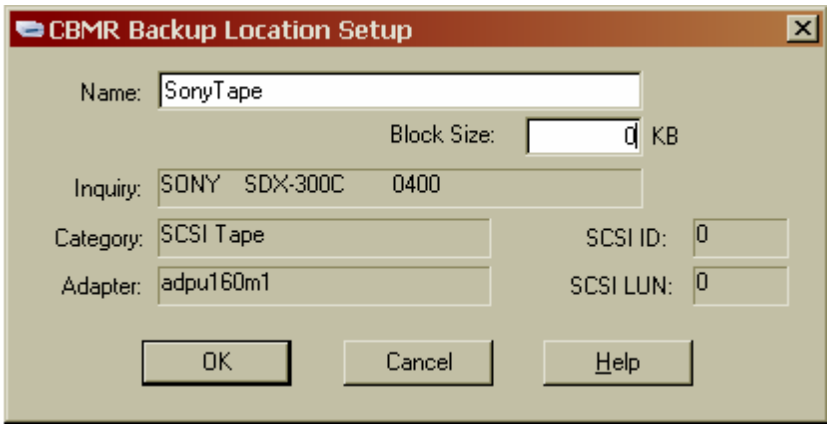
- IBM Tivoli (TSM) (needs TSM client installed)

- SEP Sesam (needs Sesam client installed)

Select an entry and press the Configure button (or double click the entry) to add this Backup Location to CBMR's known locations list. You will then be provided with the appropriate configuration dialogue.

SCSI/IDE Backup Location Setup

SCSI/IDE backup location devices can be configured using the **CBMR Backup Location Setup** dialogue. In this only the **Name** and the **Block Size** fields are editable and all other fields are for display only.



The various screen fields and their purpose are listed below.

Name	The friendly name of the backup location. Any valid character sequence up to 79 characters is acceptable The name should be unique and you cannot specify the name of an existing backup location
Block Size	The size of the tape blocks in kilobytes. Bigger block sizes will give better performance on newer tape drives However, if you are unsure, set it to 0 and CBMR will decide the appropriate block size for the device
Inquiry	The device specific SCSI/IDE Inquiry string returned from the device. May be useful to find the firmware of the device etc
Category	The category of the Backup Location. The following categories are currently supported: *SCSI Tape* *IDE Tape* *Robotics/Media Handler* *File Device (VTD)* *ITSM Module (if installed)* *Cascaded Device*
Adapter	The name of the Adapter or SCSI Port. On Windows XP, Vista, Server 2003 and Server 2008 it will give you the name of the SCSI miniport driver with a running serial number
SCSI ID	The SCSI ID or Drive number of the device
SCSI LUN	The SCSI Lun of the device - it will be 0 for IDE devices

Copyright © 1998-2014 Cristie Software Ltd.

Virtual Tape Device (VTD) Backup Location

This is a special CBMR file that can be used to emulate a tape on a disk drive. The file can be located on a removable disk, a local fixed disk or located on a remote server share.

A File backup location can be created using the **Create Backup Location** dialogue. It is possible to specify a size limit on the file itself - in which case, on reaching the specified size, an end of media condition will be created.

> *Note: ensure you do not place the VTD file on a local disk that will destroyed during a DR operation.*

Cascaded Backup Location Setup

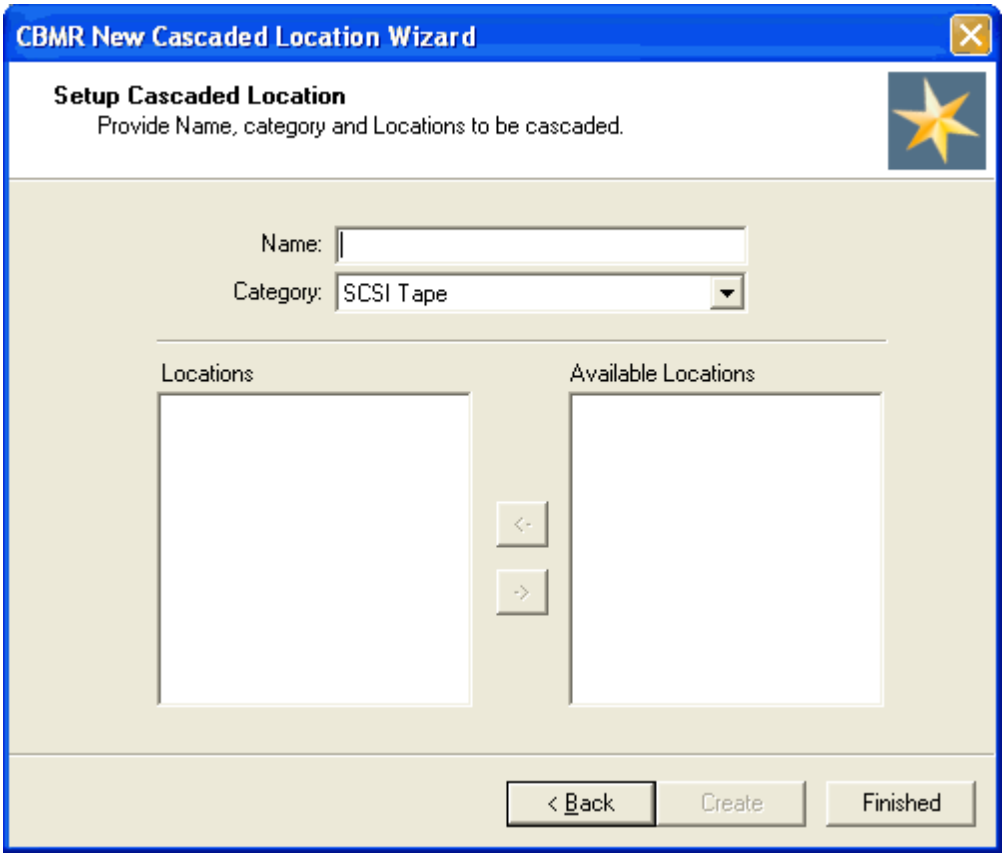
Cascaded Backup Location in CBMR are special Backup Locations which allow you to cascade two or more similar Backup Locations. Cascaded locations can be regarded as a simple library device, which eliminate the need for a media change on encountering a end-of-media condition on a device. If you have two identical tape devices attached to your system and your backup requires two media, you can cascade the two devices. The backup will continue on Device Two upon reaching the end of tape in Device One.

You can setup a Cascaded Backup Location using the **Cascaded Backup Location Setup** dialogue.

The order of the backup locations in the chain is important as the first location in the list will be accessed first.

You can double click on any location to remove it from the list and add it to the other list.

You can drag and drop using the mouse to re-arrange the locations in the **Locations** list.



The screen fields with their description are explained below:

Name	The friendly name of the backup location. Any valid character sequence up to 79 characters is acceptable The name should be unique and you cannot specify the name of an existing backup location
Category	Gives you a list of location categories in which cascading is permitted. Cascading is allowed in the following Backup Location categories: *SCSI Tape* *IDE Tape* *File Device* Changing the category will list the available locations for the category and you will lose any previous selections
Locations	Gives you a list of backup locations configured under the selected category. Highlight a location and press the [->] button to remove a location from the chain
Available Locations	Gives you a list of available locations under the selected category. Highlight a location and press the [<-] button to add it to the chain

Pressing OK will save the location and Cancel will discard the changes you have made. Pressing Help will display this topic.

> ***Note: though CBMR does not prevent you from cascading dissimilar backup location devices, for example, a DAT drive to an AIT drive, the backup operation will fail while trying to access the next backup location.***

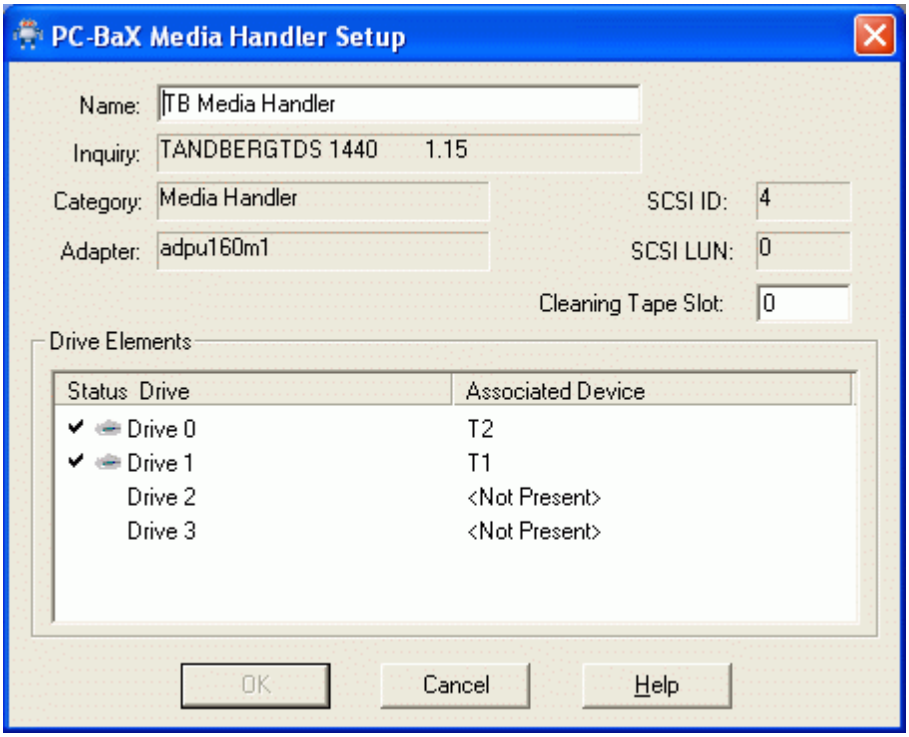
Robotics/Media Handler Setup

"Robotics" is the transport mechanism which moves the media in and out of drives and slots in a tape library device. Each drive in a library is a SCSI device by itself, which should be configured prior to this configuration. You have to make a simple association of the **Drive in the library** to the **SCSI device**. This is required because the Drive and the Robotics can be on different SCSI buses, or even on different SCSI Adapters.

> ***Note: this is a one-time setup for a Library backup location.***

A Robotics device can be configured using **Robotics/Media Handler Setup** dialogue.

Copyright © 1998-2014 Cristie Software Ltd.



The various screen fields and their purpose are listed below:

Name	The friendly name of the backup location. Any valid character sequence up to 79 characters is acceptable The name should be unique and you cannot specify the name of an existing backup location
Inquiry	The device specific SCSI/IDE Inquiry string returned from the device. May be useful to find the firmware revision of the device etc
Category	The category of the Backup Location. It will be Media Handler in this case
Adapter	The name of the Adapter or SCSI Port. On Windows XP, Vista, Server 2003 and Server 2008 it will give you the name of the SCSI miniport driver with a running serial number
SCSI ID	The SCSI ID or Drive number of the device
SCSI LUN	The SCSI Lun of the device, which will be 0 for IDE devices
Cleaning Tape Slot	Specify the Cleaning Tape Slot of the library, if any
Drives	Lists all the drives in the library/changer. The Status of the drive is shown using a tape icon. The drives are listed numerically and by the allocated Association that you have set

Pressing OK will save the Backup Location details. Pressing Help will invoke this topic.

IMPORTANT: In order to configure a Robotics device, the corresponding Library hardware should be connected and online. Ensure you choose the correct drives for the hardware. CBMR cannot know which drives are associated with the Robotics.

Once a Robotics device is configured successfully, you have to create a **Library Backup Location**, which will use this Robotics device, during backup and other media operations. Refer to Library Backup Location Setup for further details.

Note: a library backup location can only be created manually.

Library Backup Location Setup and Configuration

A Library backup location in CBMR consists of a drive, a robotics and one or more slots. It may be all or part of a physical library or autochanger. Before setting up a Library Backup Location, you must set up the individual components:

- setting up robotics (not required for autochangers)

- setting up the SCSI drives

Each library device consists of any number of available slots. Slots may not be shared between libraries, but drive devices can. For instance, if you have a library with a single drive and 20 slots, you could use the first 10 slots for Manufacturing backup and the next 10 slots for Marketing backup.

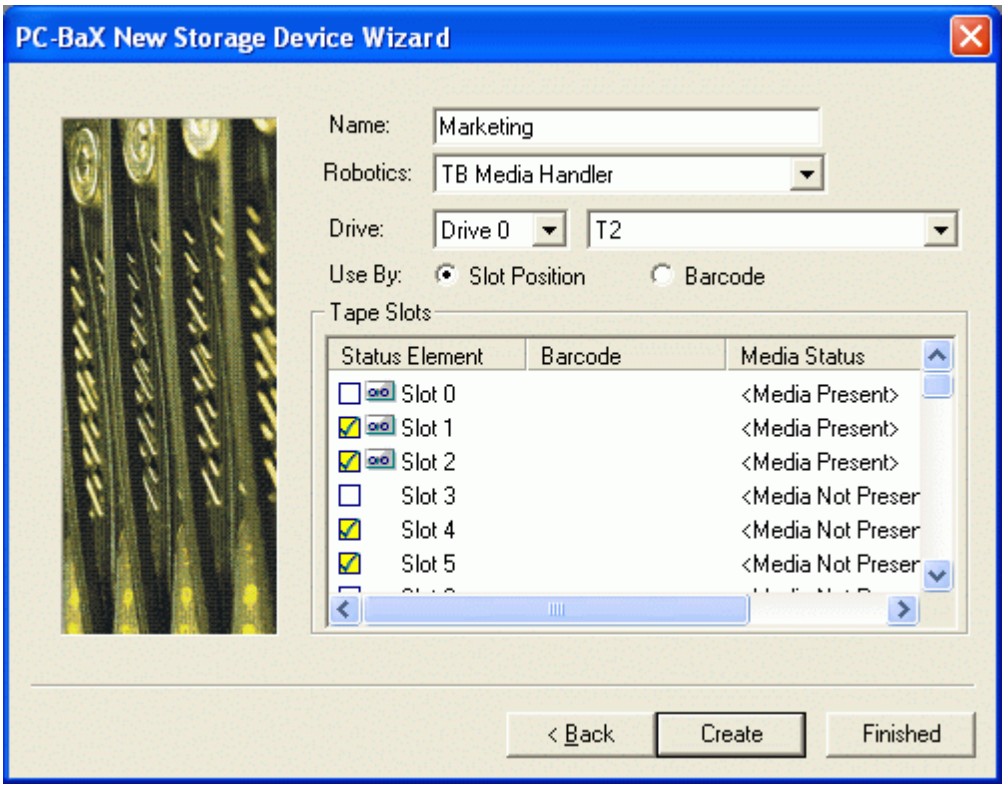
In this case, you will create one backup location with the name '*Manufacturing*' with slots 0 through 9 selected, and another with the name '*Marketing*' with slots 10 through 19 selected.

With a single device shared between two libraries, you cannot perform the 'Manufacturing' and 'Marketing' backups simultaneously. If you have two 2 drives available, each library could have its own drive, and they can be backed up in parallel.

The slots of a library device need not be contiguous. You can have slots 0, 2, 4, 5 etc. in a device configuration. In this case, the backup will continue from Slot 0 to 2 etc.

Note: you MUST have media in all the selected slots of a library device in order to use it.

This dialogue allows you to configure the **Library/Auto-loader Backup Location:**



Copyright © 1998-2014 Cristie Software Ltd.

You will specify the **Elements** or **Slots**, which will be used interchangeably in CBMR, in this dialogue.

You have to enter a friendly and unique name to the Library configuration. Single click on the box next to the slot to include that slot with this library configuration.

It is possible to select or deselect multiple slots quickly by using the Ctrl and Shift keys while highlighting the rows. A single click on any box will then select or deselect the whole selection.

You must select at least one slot for each library.

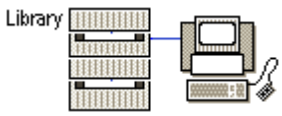
The screen fields are as follows:

Name	The friendly name of the backup location. Any valid character sequence up to 79 characters is acceptable The name should be unique and you cannot specify the name of an existing backup location
Robotics	Gives you a list of all configured Robotics devices. Select the Robotics you want to use with this definition Changing the Robotics automatically displays the Drive and Slots of the selection
Drive	The available drives in the Robotics will be listed here. Select the drive you want to use with this Backup Location definition
Use by: Slot Position	When **'Use by Slot Position'** is selected, the Media is shown ordered by Slot number. The bar code associated with each media is also shown
Use by: Barcode	When **'Use by Barcode'** is selected, the Media is shown ordered by Barcode. The Barcode order can be changed by dragging and dropping the Barcodes into the required positions
Tape Slots	Gives you a list of all available Tape Slots within the library. It also displays whether a media is present in the slot, the barcode of the media, if your device supports one Click on the box on the left of the element to select or deselect it. You must have at least one element selected in order ti use the library

Pressing OK will save the Backup Location and Cancel will discard the changes you have made. Pressing Help will display this topic.

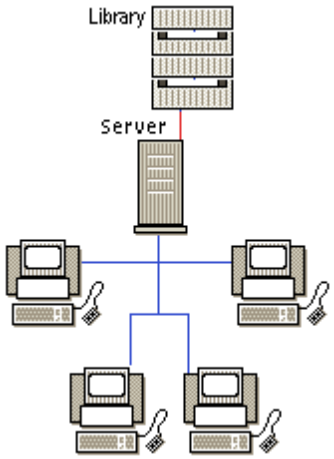
Isolated tape library example

This simple system consists of a workstation connected to a local tape library. The library consists of two SCSI drives and a robotic media handler



Simple tape library network example

This simple system consists of four workstations connected to a server. The server is connected to a local 10-slot tape library.



You could either back the workstations up to the server (as in the simple network example) and then back the server up to the tape library (as in the isolated tape library example)

In this case you could either:

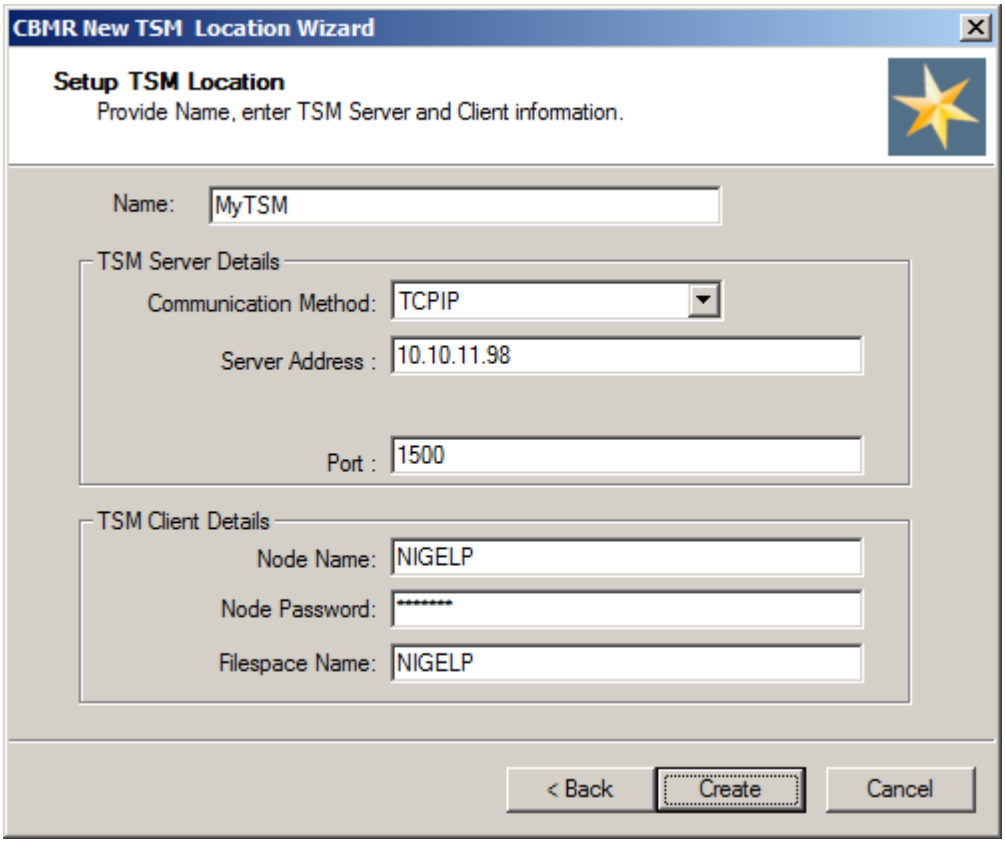
- create a single library backup location for the tape library and then back the server up to it

- create separate library backup locations for each workstation and the server in the tape library, and then back the appropriate areas of the server to the specified library backup location

TSM Backup Location Setup

CBMR TSM Backup Location Setup dialogue will enable you to define the TSM client options that CBMR should use to access the TSM server.

Copyright © 1998-2014 Cristie Software Ltd.



The various values which you can set using this dialogue are listed below:

Name	The friendly name of the backup location. Any valid character sequence up to 79 characters is acceptable The name should be unique and you cannot specify the name of an existing backup location

TSM Server Details:

Here is where you specify the communication method to be used to access the TSM server. The displayed options correspond to the currently supported options by the TSM server. The possible value combinations are listed below:

Communication Method	The method of communication to use. The possible selections are: **TCPIP** - to use TCP/IP **IPXSPX** - to use IPX/SPX **NETBIOS** - to use NetBIOS **NAMEDPIPE** - to use Named Pipes

TCPIP:

Server Address	The host name of the TSM server or the IP address in dotted decimal form
Port	The TCP port at which the TSM server is listening for client requests

IPXSPX:

Node Address	Enter the IPX/SPX node address for the TSM server
Network Address	Enter the IPX/SPX network address for the TSM server
Socket	Enter the socket number for the TSM server

NETBIOS:

NetBIOS Server Name	Enter the NetBIOS server name for the ITSM server
NetBIOS Client Name	Enter the TSM client name
LAN Adapter Number	Enter the LAN adapter number

NAMEDPIPE:

Named Pipe Name	Enter the Named Pipes server pipe name

TSM Client Details:

Here is where you will specify the name of the client node which will be used by CBMR. The node might have a password associated with it. You will also enter the name of the filespace to use. The filespace name must start with a '/'. If you haven't specified a '/' it will be added automatically.

If only single version DR backups are going to be used, the client node should be created before using TSM Administrator utilities and it must have the Backup Delete Allowed and Archive Delete Allowed set to Yes.

If backup versions are going to be used, the Node Policy domain used must be configured to use a 'versioning' copy policy.

Node Name	Enter the node name, which must have been created prior to invoking this dialogue
Node Password	Enter the node password, if any. Leave it blank for no password
Filespace Name	Enter the name of the filespace, which should start with /. If this doesn't exist before, it will be registered

Copyright © 1998-2014 Cristie Software Ltd.

Once a TSM backup location is successfully created, try to create a new header using the media utilities. If it succeeds, congratulations and your location is ready to go. If it fails, the appropriate message will tell you what is wrong.

Setting Up a Versioning Node

To set up a TSM Node to allow multiple versions of the a DR backup to be stored, follow the following steps:

- define a Management Class (MC), which contains a Backup Copy Group (BCG) and an Archive Copy Group (ACG)

- register your node to use the MC

The parameters of the BCG to be considered are:

- Versions Data Exists **2**
- Versions Data Deleted **1**
- Retain Extra Versions **30**
- Retain Only Version **60**

In this example, there can be two versions of an object. If there is more than one version and you've deleted one of them, then the deleted one will be kept for 30 days, the only remaining copy of the object will be retained for 60 days (AFTER you make it inactive).

These parameters should be set according to your preferred use of TSM.

4.2.2.2 Set a Default Backup Location

Any backup location can be used as the default location to be used in **Backup**/**Restore**/**Compare**/**Verify** jobs. The Executive window Restore, Compare and Verify always use the default backup location.

1. Select a backup location

2. Select **Set as Default Backup Location** from the **Location** top bar menu (or right mouse context menu)

The new default will be reflected in the *Backup Location* page of the **Default Settings** dialogue.

> ***Note: individual backup selection scripts can be configured to use the default backup location. By changing the default location, individual scripts will use the new location without the need to edit individual scripts.***

4.2.2.3 Viewing and Deleting Locations

Viewing Existing Backup Location Settings

Highlight the location from the **Backup Location** dialogue.

Select the **Settings** option from the Backup Location menu or double click the corresponding entry.

This will bring the corresponding setup dialogue where you can view and edit the parameters.

Deleting a Backup Location

Highlight the location to be deleted in the **Backup Locations** dialogue, and press the <Delete> key on your keyboard. Alternately you can use the Delete menu option from the **Backup Location** menu.

You will be prompted to confirm the delete operation. It is possible to delete multiple locations by selecting several locations using the <Shift> and <Ctrl> keys while making the selection.

4.2.3 Setting up CBMR for Routine Operations

Although CBMR is designed to offer a high degree of flexibility and ease of use, there may be times when you just want to configure the software to run simple routine backups with the minimum of user intervention. This section summarises the steps you can take to achieve this.

CBMR provides a number of features that should enable you to set up the system in the way that best suits you.

Scheduling routine backups
Adding jobs to the Scheduler list is an easy way of automating DR backup. The **CBMR Scheduler** offers a comprehensive time/date setup and the choice of running with **Backup Selection** scripts or for even greater flexibility, command files.

Customising the User Interface
You can simplify the appearance of CBMR by hiding some of the options, for example, *Backup Locations* and *Default Settings* in the Configuration drop-down menu. The **pcbax.ini** file can be edited to remove any of the main window objects. The list of variables in the **pcbax.ini** file controls what appears on the CBMR launch panel. All the variable names are relevant to their function, so it is easy to decide which you need to change if required.

To hide an object, set the appropriate '*Showxxx*' value to zero. For example, to hide the *Backup Locations* object, set:

ShowBackupLocations = 0

4.3 Introduction to Backing up data

The purpose of a backup is:

- to minimise the effect of lost data be it due to human error or machine error
- maintain an archive copy

One of the main tasks in creating a backup is ensuring that there is an up-to-date copy of all data. This does not mean backing up every file every time. Although a complete and full backup is necessary, in between times a selective backup is enough to ensure that all data is secure up to the last backup.

Backing up your data using CBMR is very easy:

- Create some Backup Selection scripts to cover the routine jobs such as a full weekly backup, a daily incremental backup and so on.
- Pick the appropriate Backup Selection script and set the Backup in motion.

You can also set up the Scheduler to run the jobs automatically at the set times.

See also the Backup Strategy topic in this document.

Copyright © 1998-2014 Cristie Software Ltd.

4.3.1 Backup Schedules and Selection Scripts

Backup Schedules and **Selection Scripts** are used to define a set of instructions relating to a Backup. The scripts contain the data tagged for backup, the rules to follow during the operation, and header information. Existing scripts can be viewed, modified or deleted as requirements change. The scripts can be temporary and used for a one off job, or can be saved and used as and when required. Once saved you can view, modify or delete them as your requirements change.

Once you have established some backup routines and know what you need to backup and when, it is a good idea to create a range of scripts covering all the routine backup jobs.

CBMR is supplied with a pre-defined script called 'Backup all files on system [Boot] drive'.

From the main Backup Schedules drop-down menu you can change the **View** (icons, list or details display) and **Sort** by name/date. Also, from the **Jobs** menu you can perform all the routine tasks such as **Modify** an existing schedule, **Run** a selected schedule, **Delete** a schedule, create a new schedule (**Create New**) and access the **Default Settings**.

If the **Details** view is displayed, you can also sort the entries in **Description**, **File Name** or **Date/ Time** sequence by clicking in the appropriate column heading.

4.3.1.1 Creating a Backup Schedule

To create a new DR backup schedule/script, select the **Run or Schedule Disaster Recovery Backup** option from the main menu.

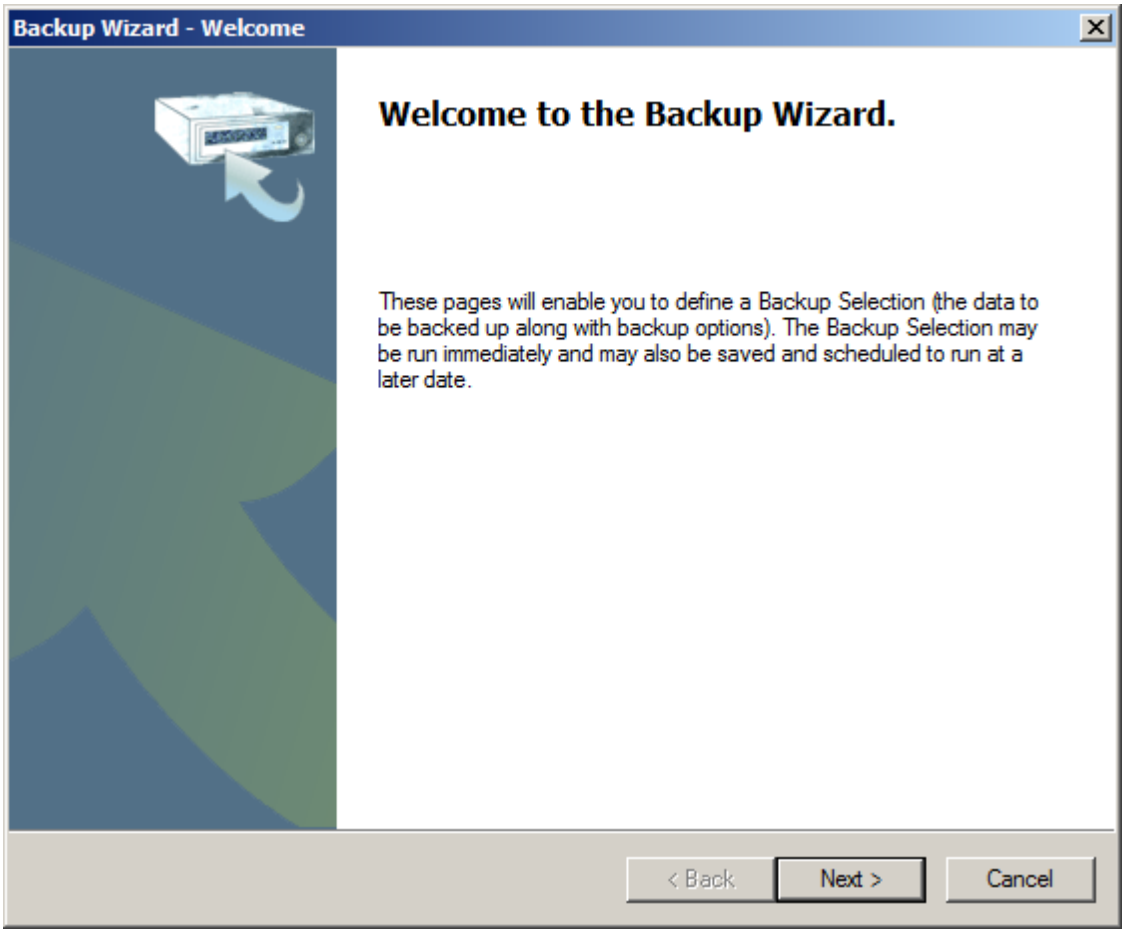
This can also be located via:

- the **Tool** top bar menu in the Backup Selections tool

- double click the **Create New** icon in the Backup Schedules drop-down menu

- double click the **Backup Now** option in the Tools drop-down menu

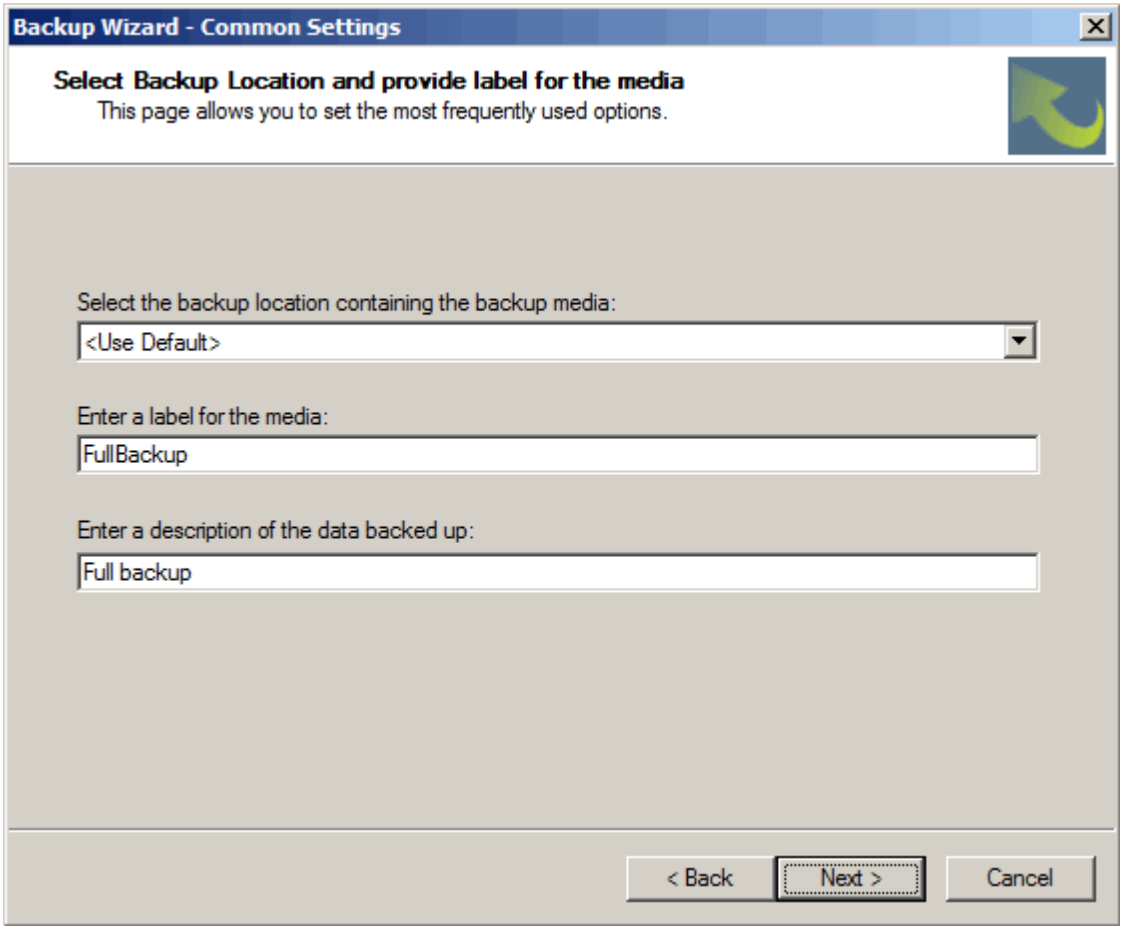
Any one of these methods will invoke the Backup wizard. This will take you through the steps required to create the new Backup Selection script.


Backup Wizard - Welcome
Welcome to the Backup Wizard.
These pages will enable you to define a Backup Selection (the data to be backed up along with backup options). The Backup Selection may be run immediately and may also be saved and scheduled to run at a later date.
< Back
Next >
Cancel

This wizard will guide you through the process of creating the rules governing a backup. The Selection script produced can be run immediately or saved for future use and a schedule can be set up to run the saved script automatically.

Copyright © 1998-2014 Cristie Software Ltd.

Common Settings


Backup Wizard - Common Settings
Select Backup Location and provide label for the media
This page allows you to set the most frequently used options.
Select the backup location containing the backup media:
<Use Default>
Enter a label for the media:
FullBackup
Enter a description of the data backed up:
Full backup
< Back
Next >
Cancel

Backup Location field:

Gives the option to use the Default Backup Location or any other connected Backup Location.

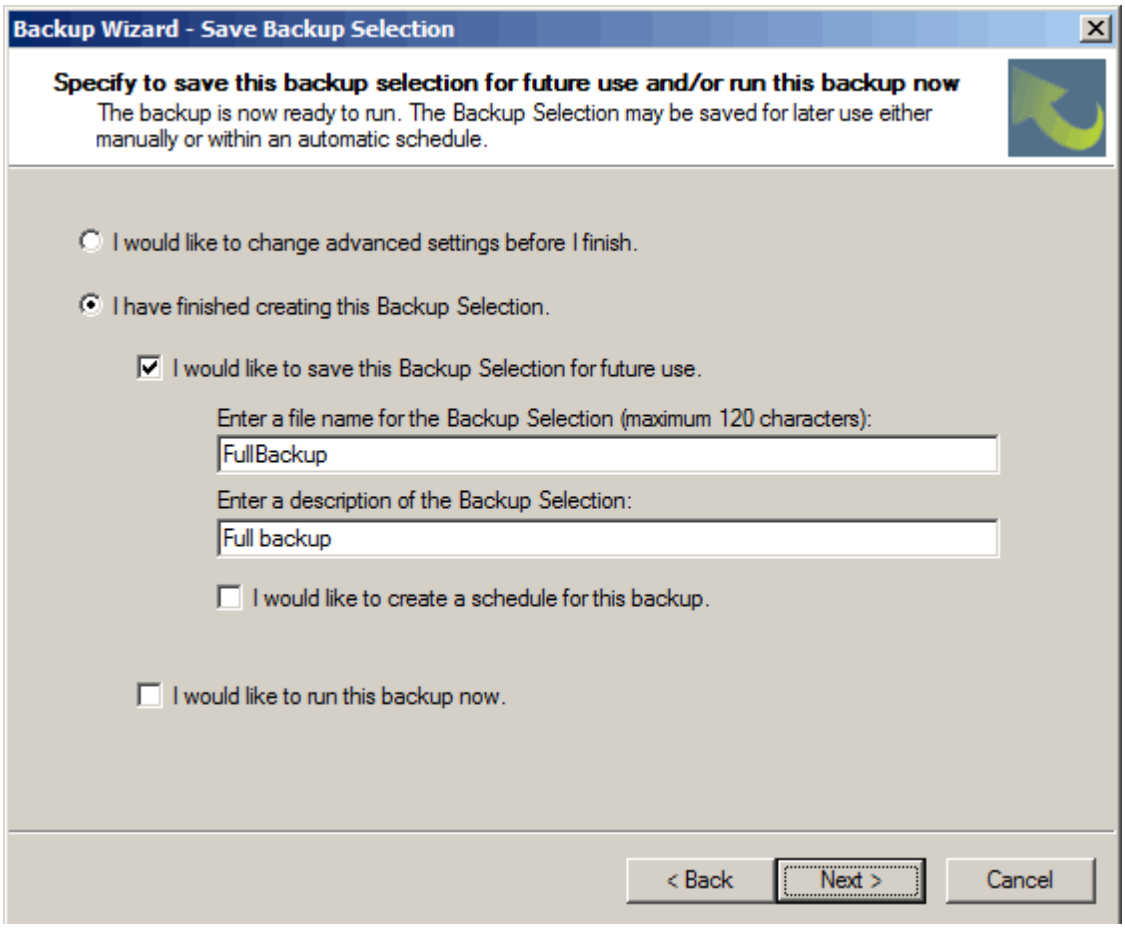
Media Label field:

The media label is a unique identifier for the media loaded in your Backup Location. Ideally the label should reflect the contents of the media. If you need to Restore data, especially in an emergency, headers such as 'Volume 1' and 'Volume 2', without any other description, do not mean anything and will cause a lot of frustration.

Data Description field:

The data description field allows you to add more specific details, which may be useful in identifying the contents of the tape. It may not be you who is accessing it, perhaps several months from now.

Save Backup Selection Script


Backup Wizard - Save Backup Selection
Specify to save this backup selection for future use and/or run this backup now
The backup is now ready to run. The Backup Selection may be saved for later use either manually or within an automatic schedule.
I would like to change advanced settings before I finish.
I have finished creating this Backup Selection.
I would like to save this Backup Selection for future use.
Enter a file name for the Backup Selection (maximum 120 characters):
FullBackup
Enter a description of the Backup Selection:
Full backup
I would like to create a schedule for this backup.
I would like to run this backup now.
< Back
Next >
Cancel

This page is displayed after the most common backup options have been set. If more advanced options need to be set, then choose the **Advanced Settings** option and this dialogue will be presented again at the end.

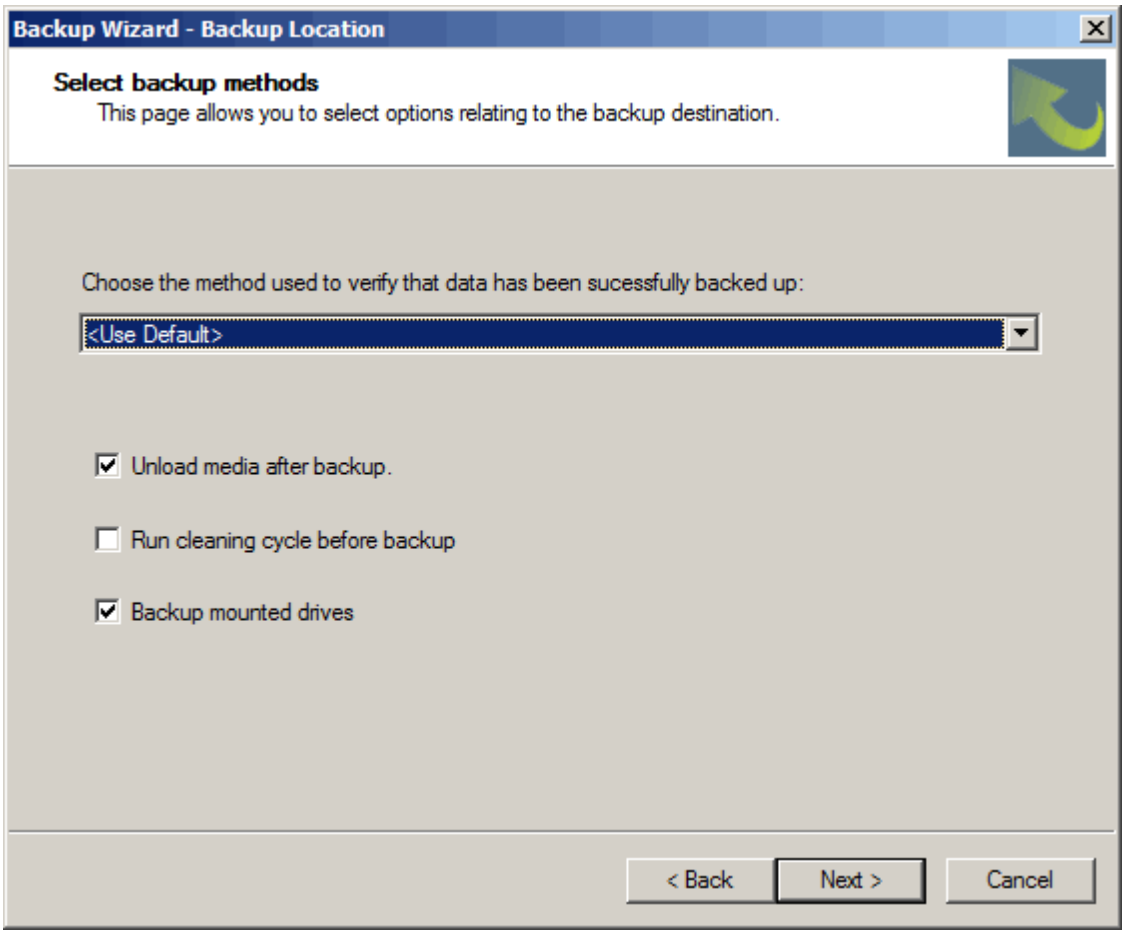
In order to save the backup script, a file name and description must be given. The name must not be more than eight characters and is use to create a script file. The description will be used to identify the script in the **Backup Scripts Tool**, so it make sense to make this meaningful.

It is not necessary to save the backup script if you only want to run it immediately.

If the option to create a schedule is selected, then the schedule dialogues will be presented after the script file has been saved. If CBMR has been configured to use the Microsoft Task Scheduler, then the Task Scheduler Wizard will be presented, otherwise the CBMR Task Scheduler property sheet will be presented. In either case, the options required to run the newly-created script file will already be filled in.

Copyright © 1998-2014 Cristie Software Ltd.

Backup Location


Backup Wizard - Backup Location
Select backup methods
This page allows you to select options relating to the backup destination.
Choose the method used to verify that data has been sucessfully backed up:
<Use Default>
Unload media after backup.
Run cleaning cycle before backup
Backup mounted drives
< Back
Next >
Cancel

This page allows you to set various options relating to the way the backup is stored on the destination **Backup Location**.

Verify Method

- **<Use Default>** - use the default verifiy method set in Default Settings
- **Verify After Backup** - checks the validity of the recorded media
- **None** - does not perform any checks
- **Check Integrity Alone** - after finishing the backup, the media will be scanned from the beginning to end, ensuring it is readable
- **Byte By Byte Comparison** - after finishing the backup, each file on the media will be compared against its disk counterpart and the differences reported

Unload Media

If the Backup Location supports automatic ejection of the media, then this option will ensure that the media is unloaded at the end of the backup cycle.

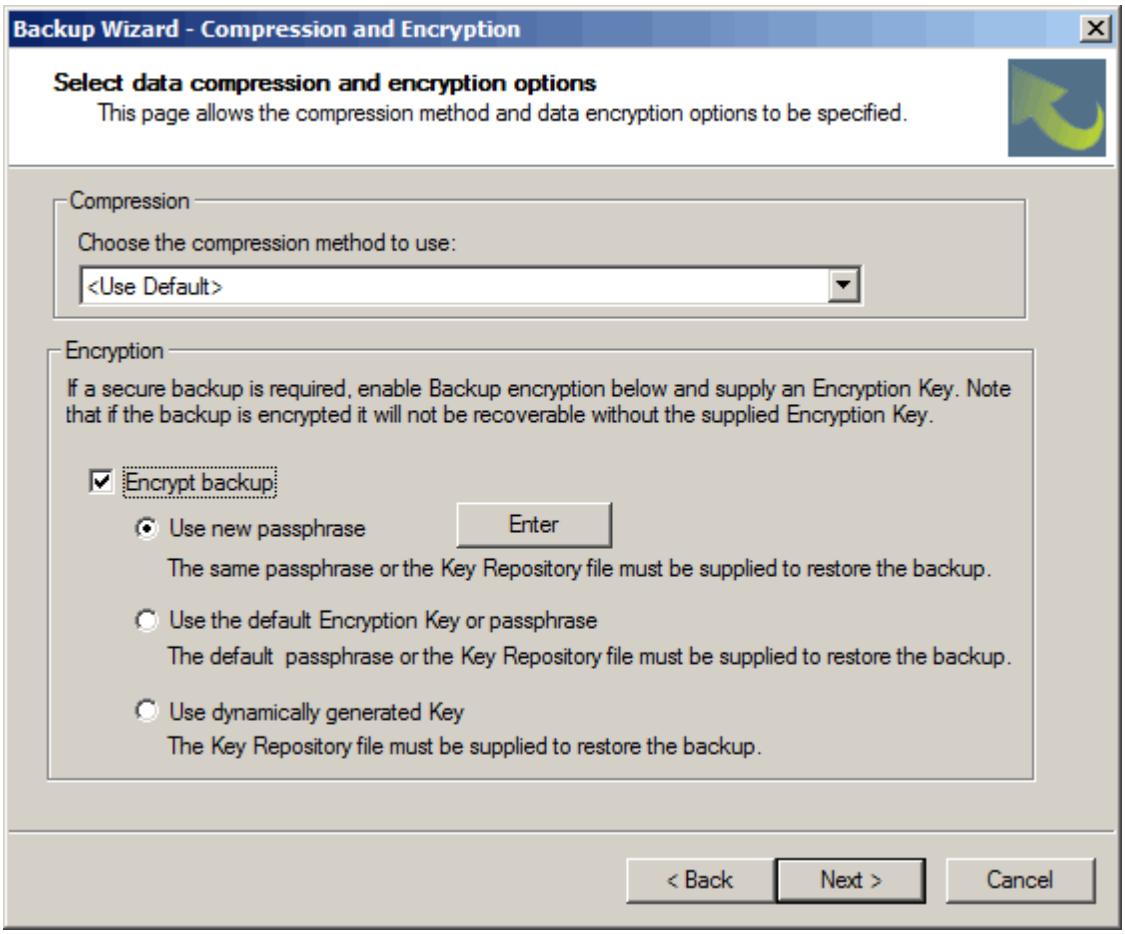
Run Cleaning Cycle

If the Backup Location is a library or autochanger that supports a cleaning media, this option ensures that a cleaning cycle is completed before the backup commences.

Backup mounted drives

Include any mounted drives (partitions) in the backup.

Compression and Encryption


Backup Wizard - Compression and Encryption
Select data compression and encryption options
This page allows the compression method and data encryption options to be specified.
Compression
Choose the compression method to use:
<Use Default>
Encryption
If a secure backup is required, enable Backup encryption below and supply an Encryption Key. Note that if the backup is encrypted it will not be recoverable without the supplied Encryption Key.
Encrypt backup
Use new passphrase
Enter
The same passphrase or the Key Repository file must be supplied to restore the backup.
Use the default Encryption Key or passphrase
The default passphrase or the Key Repository file must be supplied to restore the backup.
Use dynamically generated Key
The Key Repository file must be supplied to restore the backup.
< Back
Next >
Cancel

Compression

Allows the compression method to be selected for the backup. Options are:

- **<Use Default>** - use default compression method selected in Default Settings
- **None** - data is not compressed
- **Software** - data compression will be performed by the CBMR software before the data is written to the Backup Location
- **Hardware compression (if available, otherwise none)** - this option will attempt to make the Backup Location perform the data compression. If compression is not available on the hardware, the data will remain uncompressed
- **Hardware compression (if available, otherwise Software)** - by preference, data compression will be performed by the hardware if it is possible, otherwise compression will be done by CBMR software

Encryption

Enables encryption for the backup. An entry will then be made in the **Key Repository** file for the backup. Options are:

- **Use new passphrase** - select this option and enter a new passphrase for the backup. The

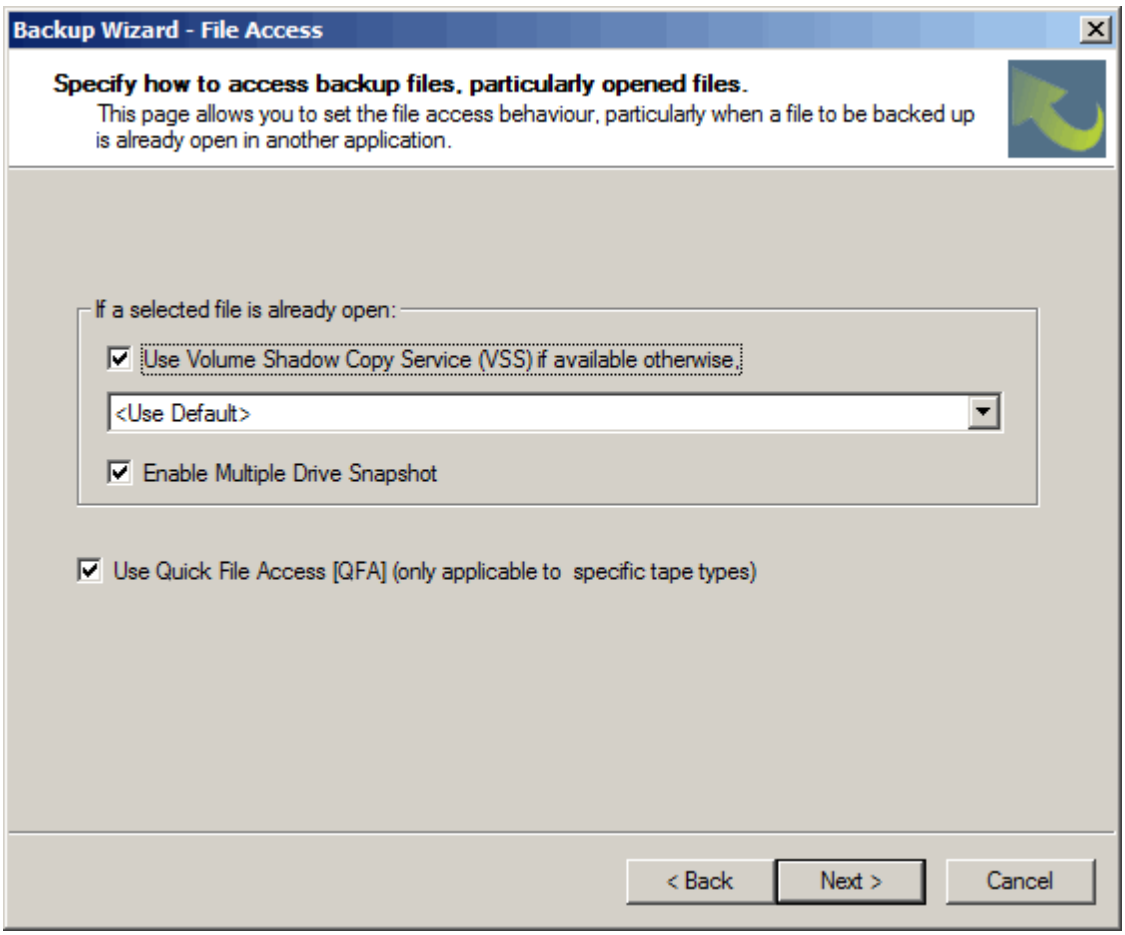
Copyright © 1998-2014 Cristie Software Ltd.

resulting passphrase will generate a new Key for the backup. The Key (not the passphrase) is saved in the Key Repository file. To restore the backup the entered passphrase or the Key Repository file must be accessible

- **Use the default Encryption Key or passphrase** - instead of specifying a new passphrase, use the currently defined default value for the backup. An entry for the default Key will already be in the Key Repository file. To restore the backup, the default passphrase or the Key Repository file must be accessible
- **Use dynamically generated Key** - a new key will be generated randomly (no passphrase is used here) just before the backup is started. The random key is then saved to the Key Repository file. To restore the backup, the Key Repository file must be accessible

Please refer to the Backup Encryption topic for more details.

File Access


Backup Wizard - File Access
Specify how to access backup files, particularly opened files.
This page allows you to set the file access behaviour, particularly when a file to be backed up is already open in another application.
If a selected file is already open:
Use Volume Shadow Copy Service (VSS) if available otherwise
<Use Default>
Enable Multiple Drive Snapshot
Use Quick File Access [QFA] (only applicable to specific tape types)
< Back
Next >
Cancel

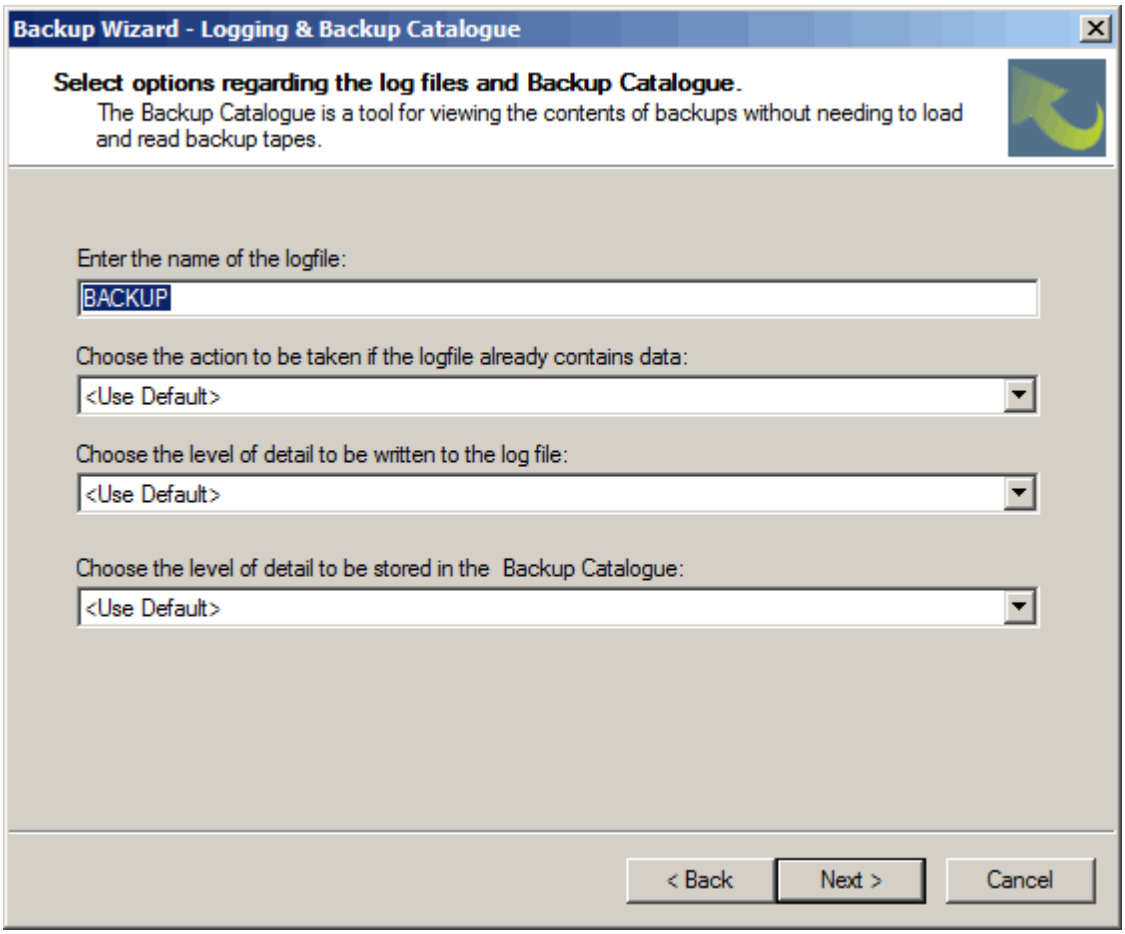
If a selected file is already open

Allows you to specify whether to use Microsoft VSS to back up open files and what action to take when open files are encountered and VSS is not being used. If you are using VSS, then Multiple Drive Monitoring can also be selected.

Use Quick File Access (QFA)

This option, if selected, will provide rapid access to files during a restore operation. (Not all drives support this option.)

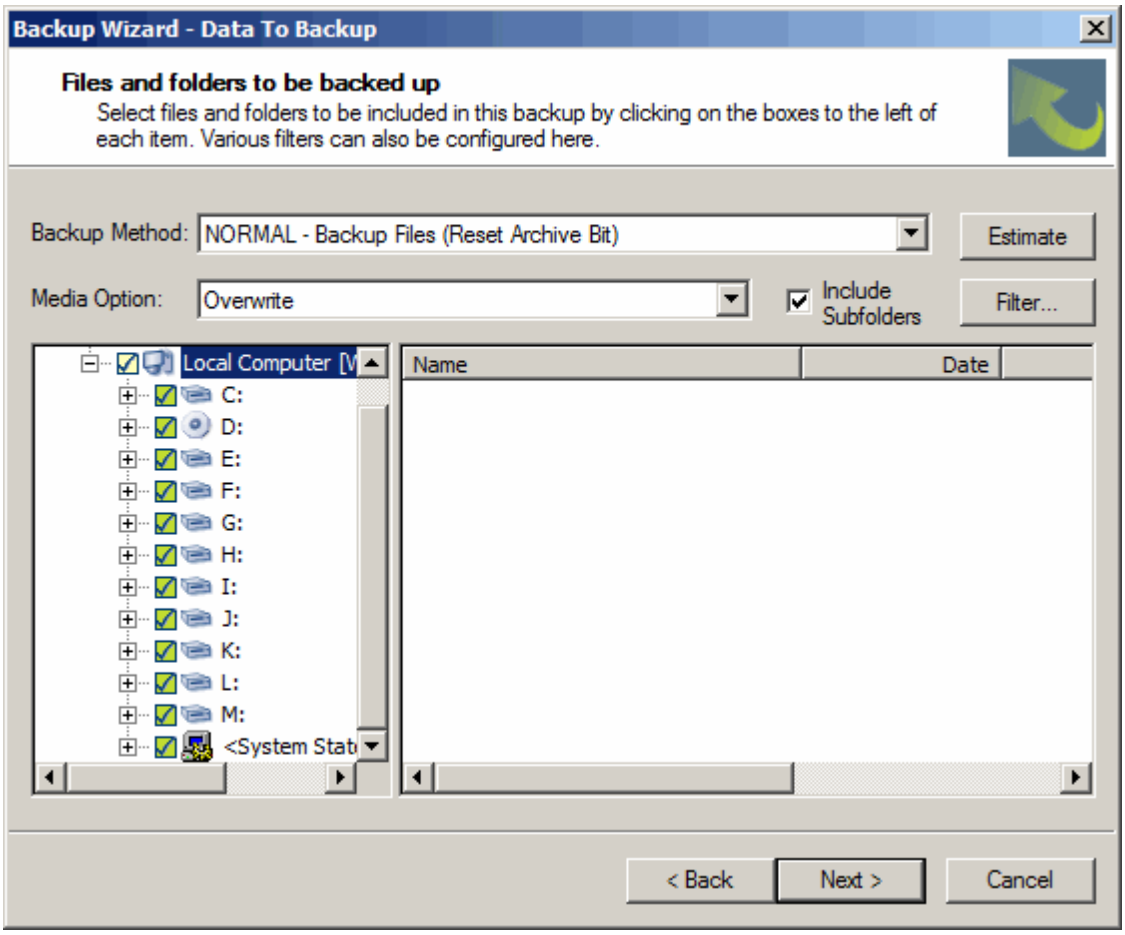
Logging and Backup Catalogue



This page allows you to set options regarding the information that is stored in the backup log file and that stored in the **Backup Catalogue**.

Copyright © 1998-2014 Cristie Software Ltd.

4.3.1.2 Backup Wizard - Data To Backup



On this page, you will select the data to be backed up and the most common options.

Specify what you want to include in the backup in the **Data To Backup** window. It can be a straightforward backup of all files in the selected drive(s) (servers/workstations on the network) or a more selective backup where you have de-selected certain directories/files and/or set restrictions on files.

The **Data To Backup** displays two separate items under the **Desktop** icon:

- The Local Computer
- The Network

Local Computer

The Local Computer contains the logical drives available for backup. The floppy drive will also be included if there is a disk in the drive at the time the Backup property page is opened.

> ***Note: System State is listed as a separate entity. To include the complete System State contents in the backup, click the System State box.***

Network

The Network contains the available Network Providers (types of network) on your system:

- Microsoft Windows Network (expands to show each domain and workgroup)
- NetWare or compatible network (expands to show each NetWare file server)
- User defined shares (expands to show shares residing on other platforms such as LANserver. These must be added manually)

A single click on a +/ - expands/collapses an item.

A single click on a white box selects/de-selects the contents (of a drive, directory or server for example).

Double click an item label to expand/collapse an item.

A tick in the grey box indicates that at least **one item** is selected for backup; it does **NOT** mean that every item underneath is selected.

Backup Method For Files

There are four pre-configured backup methods to choose from.

NORMAL - Backup Files (Reset Archive Bit)

The Normal selection will backup all the selected files and reset the archive bit

COPY - Backup Files

The Copy selection will backup all the selected files without affecting the archive bit

DIFFERENTIAL - Backup Changed Files

The Differential selection will backup all files that have changed or are new since the last Normal or Incremental backup. The backup will not affect the archive bit

INCREMENTAL - Backup Changed Files (Reset Archive Bit)

The Incremental selection will backup all files that have changed or are new since the last Normal or Incremental backup. The backup will reset the archive bit

Media Options

The media options control the way that data is written to the media.

Overwrite - If overwrite is selected the backup will start at the beginning of the media overwriting any existing data

Overwrite media with the same label, append otherwise - Selects overwrite only if the media label matches with the requested media, otherwise the data will be appended to the media

Overwrite media with the same label, fail otherwise - Selects overwrite only if the media label matches with the requested media, otherwise the operation fails and no data will be written to the media

Append, overwrite if not appendable - Selects append, but if the media is blank or the media contains a non CBMR data set and therefore cannot be appended, the media is overwritten

Append to media with the same label, fail otherwise - Selects append only if the media label matches with the requested media, otherwise the operation fails and no data will be written to the media

Include Subfolders

When this option is ticked, selecting an item in the tree view will also select everything below that item in the tree.

Filter

The **Filter** option will display the *File Restriction Settings* dialogue which allows you to be very precise about what is included/excluded in the backup.

Estimate

The **Estimate** option displays a window containing an estimate of the size of the backup you have

Copyright © 1998-2014 Cristie Software Ltd.

defined (the number of files and the size in Bytes). This could be useful if you need to know in advance how much capacity you require for this backup or estimate how long the job will take to run.

See also the Configure Backup Properties page for additional details.

System State

The *Data to Backup* page displays the logical drives available for backup on the local computer. The floppy drive will be included if there is a disk in the drive at the time the Backup property page is opened.

The **System State**, which includes the **Registry**, **Boot Files** and **Com+ Registration** database, is listed as a separate directory to make it easy to ensure that the complete contents can be included in the backup

If you wanted to run a one-off backup without saving the Backup Selection script, you can make your selections on this screen and press the **Backup** button.

The display is a hierarchical structure in the same style as the Windows Explorer window.

A single click on a +/ - expands/collapses an item.

+ A plus sign indicates that a directory has not been fully expanded.

- A minus sign indicates that a directory has been expanded to its lower level.

Selecting Network Shares

The selection process for selecting network shares is just the same as for a local drive.

The Network contains the available **Network Providers**, typically Microsoft Windows Network, NetWare or Compatible Network and User Defined Shares.

Microsoft Windows Network

Click on Microsoft Windows Network '+' box to display all the available domains.

Select a domain '+' box to display all available servers.

You can then either:

click on the clear box attached to a server to select all shares on that server
or
click on a server '+' box to list the shares and proceed to select individual shares by clicking the clear box attached to the relevant share.

> ***Note1: once an entity has been selected, even if it is only one file, the grey box attached to the network provider, the Network label and the Desktop will be ticked.***

> ***Note2: when Windows is started it creates administrative shares for each local drive. They are identified by a dollar sign - for example C$, D$. Only members of the Administrators, Backup Operators or Server Operators Group can backup these shares.***

NetWare or Compatible Network

Click on NetWare or Compatible Network '+' box to display all the available fileservers.

Select a fileserver '+' box to display all the available volumes.

You can then either:

click on the clear box attached to a volume to select all directories/files
or
double click on the volume label to list the directories/files and proceed to select individual directories or files.

> *Note: once an entity has been selected, even if it is only one file, the grey box attached to the network provider, the Network label and the Desktop will be ticked.*

User Defined Shares

Select the User Defined Shares '+' box to display all available shares.

Then you can either

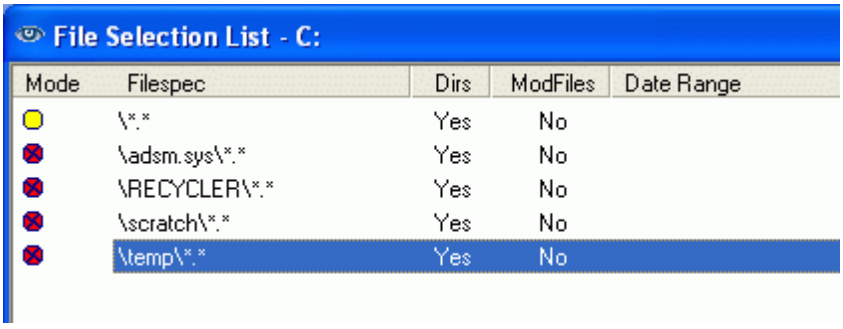
click on the clear box attached to a share to select all directories/files
or
double click on the share label to list the directories/files and proceed to select individual directories or files.

Set Attach Info

This dialogue allows you to assign a user name and password to attach to the selected resource. The resource name is displayed in the dialogue title.

File Selection List

The **File Selection List** window lists the selections you have made in the directory tree. Those with a green circle are included in the process (Backup, Restore, Compare or Verify). A cross (x) in a red circle indicates that sub-directories/files have been excluded.



You can **Modify** any item in the list and **Add** or **Delete** entries via the *File Selection* dialogue.

File Selection Dialogue

The **File Selection** dialogue allows you to change the restrictions of the selected file or modify an existing specification. CBMR will accept wildcard ***** and **?** definitions. For example:

Statement	Result
.	All files in the Root directory

Copyright © 1998-2014 Cristie Software Ltd.

\windows\doc*.doc	All files in the windows directory with a .doc extension
\icons?.bmp	All files in a range eg **icons1.bmp**, **icons2.bmp** and so on

You can also apply date restrictions (ignore files Before/After), Include sub directories or Modified files only.

Selecting Network Shares or Volumes

This section describes the selection of network servers and shares, and highlights actions which are specific to this process. The basic principles of expanding/collapsing a network, tagging/untagging items for backup and adding dataset details are exactly the same as for local drives but there are access issues which are important when making connections to network servers and volumes.

Some shares residing on other platforms such as LanManager or LANserver will not be included in the network hierarchy.

Microsoft Windows Network

Expanding the **Microsoft Windows Network** displays a list of domains. Expanding a domain lists the servers belonging to that domain. It is only at the server listing level that you can begin to the selection process (indicated by the clear check box attached to each item).

Click on a domain '+' box to display all the available servers

Then, either click on the clear check box attached to a server to select all shares on that server

or

click on a server '+' box to list the shares and proceed to select individual shares by clicking the clear box attached to the relevant share.

> *Note: once an entity has been selected, even if it is only one file, the grey box attached to the network provider, the Network label and the Desktop will be ticked.*

NetWare or Compatible Network

CBMR supports Windows supported networks such as the Novell NetWare network operating system.

Expanding the NetWare Network displays a list of file servers attached to that network.

Click on the clear check box attached to a server to backup all volumes on that server

or

Expand the server to list the shares and proceed to select individual shares by clicking the clear box attached to the relevant share.

> *Note: once an entity has been selected, even if it is only one file, the grey box attached to the network provider, the Network label and the Desktop will be ticked.*

Creating User Defined Shares

The **'User Defined Shares'** provider is used to list shares on other platforms such as LANserver or LanManager. Although these shares may be accessed, they are not automatically available for selection. They must be added manually.

Creating User Defined Shares

User defined shares are specified in a separate file called **usershar.ini** located in the **\pcbax** directory. Below is an example entry:

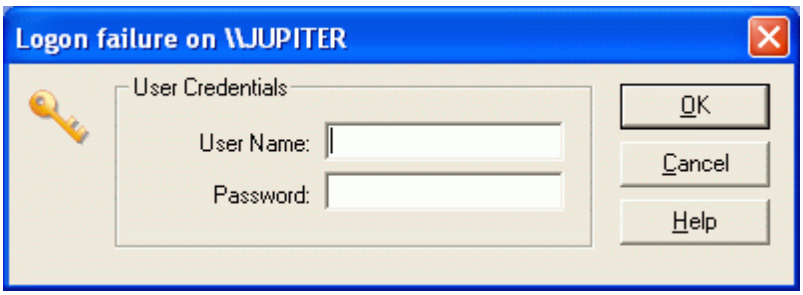
Syntax

```
[main]
\\DEV\dev_files
\\DEV\documents
```

Logon Failure

CBMR automatically tries to create any connection required to access a resource. The user account (name and password) can be specified either as a default account or a different account for an individual resource.

When CBMR tries to make a connection to a resource, it checks in **userinfo.ini** to see if it already has a connection saved in the file. Initially it checks for a default user account name and password, if it does not find one it checks for a server/machine level account and, finally, a share account. If no connection is found, then the *'Logon failure at <UNC path>* dialogue is displayed.



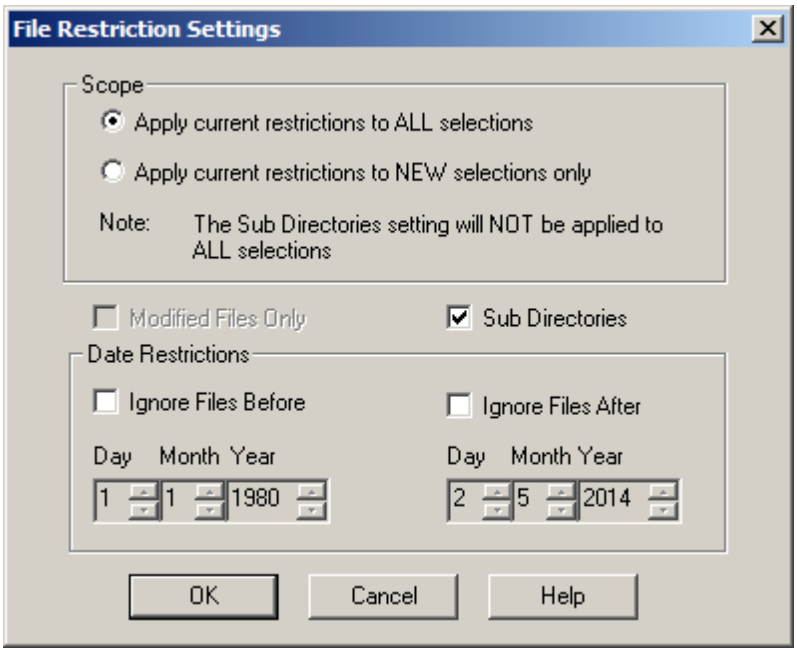
You must provide a user name and password which has permission to access this account.

Any connection made via this route is used for this access only and will not be saved when the program exits.

Copyright © 1998-2014 Cristie Software Ltd.

Applying File Restrictions

The *File Restriction Settings* dialogue (**Set Restrictions** option in the **Selections** top bar menu in CBMR Backup Selections script properties) allows you to be very precise about what is included/ excluded in the backup.



You can apply the following restrictions:

Sub Directories	A tick in this box means that all sub directories are included.
Modified Files Only	A tick in this box means that only modified files are included.
Ignore Files Before	A tick in this box means that files created before the date specified in the calendar are excluded.
Ignore Files After	A tick in this box means that files created after the date specified in the calendar are excluded.

A tick in both both boxes (Ignore Files Before/After) will restrict the backup to files within the dates specified.

Any restrictions you have set can be applied to the entire backup or only to selections made from this point onwards.

File Restriction Settings

This window allows you to define restrictions which will apply to all selected drives on this backup.

You can restrict the selection by:

- Including/Excluding Sub Directories

when the **Sub Directories** box is ticked, all sub directories will be included in the backup

- Including/Excluding Modified Files

when the **Modified Files Only** box is ticked, then only those files which have a modified flag set will be backed up

- Excluding Files According to Date

select the **Ignore Files Before** or **Ignore Files After** options. Using either of these options, you can exclude files before or after a specified date

- Including Files According to Date

if you want to restrict the backup to files within a particular date range, then set dates for both 'Ignore Files Before' and 'Ignore Files After'

The **Scope** options give you the choice of:

applying these restrictions to all selections in current Backup Selection script (current and future)

or

only applying them to selections tagged from this point onwards

4.3.1.3 Viewing and Modifying Existing Backup Selection Scripts

Viewing Existing Backup Selection Scripts

To display existing Backup Selection scripts, click on the Backup Selection button on the toolbar or select Backup Selections from the **Tools** top menu.

- **View** - provides different display options, such as Large/Small icons, a List or a Detailed view. The Details View provides some extra information about the scripts. It details the name (the entry in the *Description* line), the filename (the entry in the *File* line) and the date/time created
- **Sort** - allows you to arrange the scripts in alphabetic sequence (**Sort by Name**) or in date sequence (**Sort by Date**). When in Details view, you can also sort the scripts by clicking in the column headings
- **Script** - contains all the operations you might perform on a script. For example, **Modify**, **Delete**, **Create New**

There is a pre-defined script supplied with CBMR called 'Backup all files on system [Boot] drive' (filename - **system.scp**). When you run this script, the system identifies which drive the Operating System was booted from and backs up all the files on that drive. This means that should there be a need to recover the system, you have a copy of all your system files.

Modifying an Existing Selection Script

Open the **Backup Selections tool.**

Double click on the script that you want to change or highlight it (single click) and select **Modify** from the **Script** top bar menu.

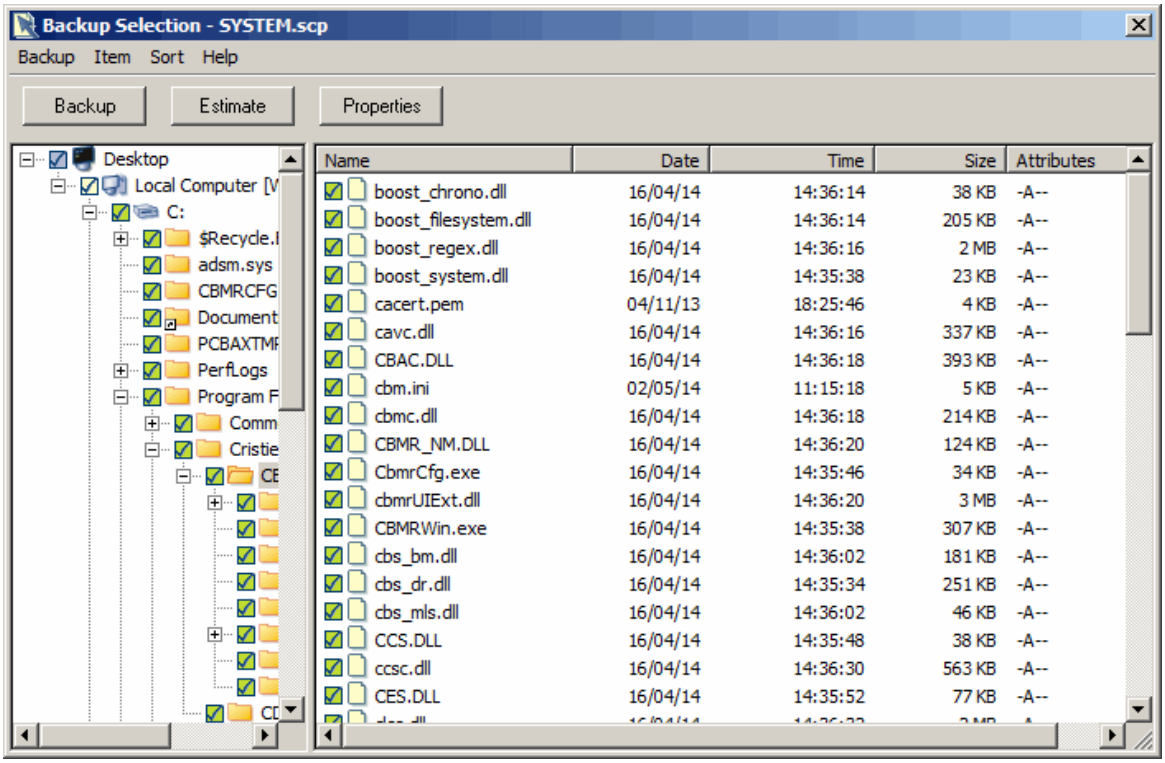
Make the changes to the selections (file changes/Backup options etc).

Select **Save** from the top bar menu and press OK to close the script window.

If you decide not to save the changes you have just made, select the Cancel button.

Copyright © 1998-2014 Cristie Software Ltd.

4.3.1.4 Backup Selection Script Editor



The backup selection script editor is where you select the data to be backed up and set other properties relating to the backup. On the main screen, you can select (tag) the data to be backed up. There are also buttons to begin the backup immediately, estimate the size of the backup and set further properties including the file name used to store the backup selection script.

The **Backup** menu provides options to alter the backup's **Properties**, set **Restrictions** on whether the tagged data is included in the backup (for example based on the age of a tagged file), estimate the **Size** of the tagged data, run the **Backup** immediately, **Save** the script and **Close** the Backup Selection script editor.

The **Item** menu (which is also available as a context menu) allows you to view the **Dataset** details for a drive, **Tag** or **Untag** an item and view a **Selection List** for a drive. In the Enterprise version of CBMR, this menu also enables you to set usernames and passwords for attaching to network drives.

The **Sort** menu is available when at least one item is highlighted in the file list view. It enables the file list to be sorted in a variety of ways. The file list can also be sorted by clicking on the list's column headers.

Backup Options Page

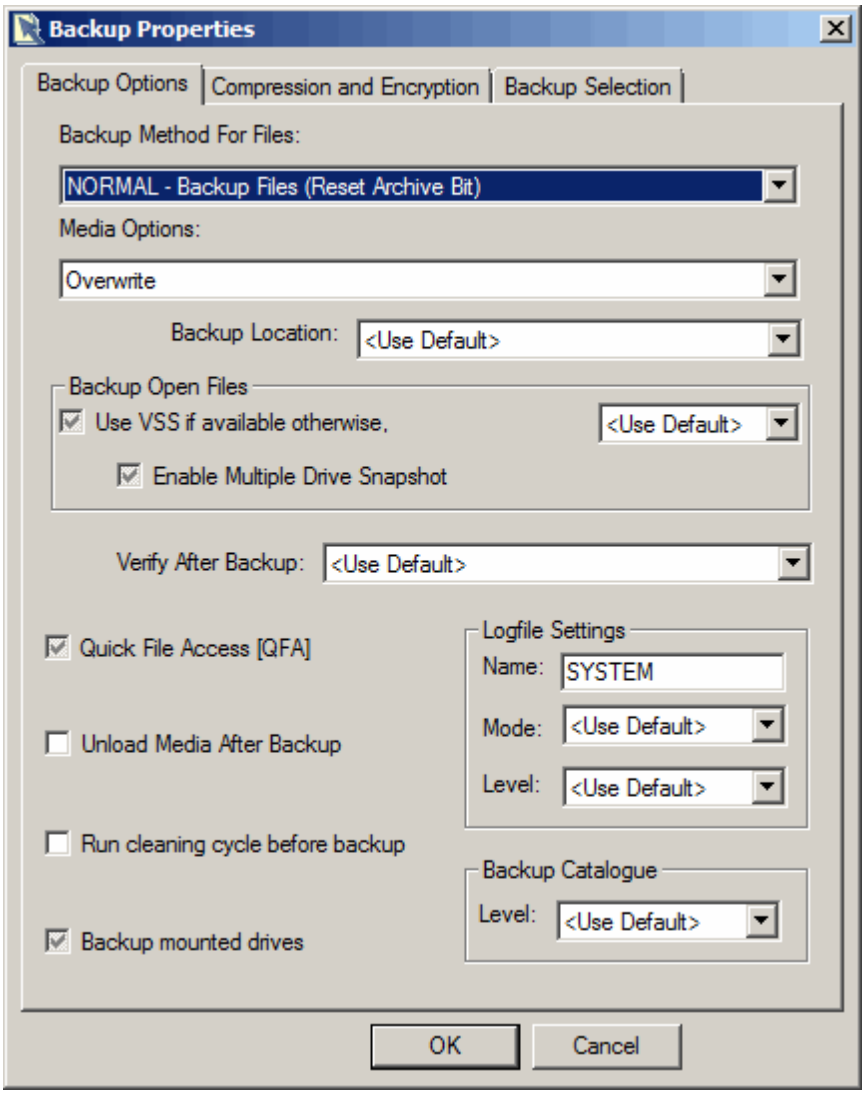
The options on this page allow you to define a set of actions which CBMR will carry out before, during and after the backup.

For example:

- what backup method will you use?
- is this backup going to append or overwrite an existing backup?
- what Backup Location is the backup going to be written to?
- do you want to apply data compression?
- do you want to run the Compare program automatically after the backup has finished?

- do you want a log file created?
- would you like an entry made in the Backup Catalogue?

Initially the options will be set to <Use Default>, which means whatever is set in Default Settings property pages will be used for this job. If necessary you can make some adjustments to suit the current job. **Any changes made here only apply to the current backup selection script and do not alter the Default Settings properties.**



For descriptions of most of the fields please refer to the Backup page of the Default Settings section in this document for a brief description of the fields.

The remaining fields are:

Backup Location - gives the option to use the Default Location or any other connected Location (storage device)

Unload Media After Backup - if the Backup Location supports automatic ejection of the media, then this option will ensure that the media is unloaded at the end of the backup cycle

Run cleaning cycle before backup - if the Backup Location is a library or autochanger that supports a cleaning media, this option ensures that a cleaning cyle is completed before the backup commences

Backup mounted drives - include any mounted drives (partitions) during the backup

Copyright © 1998-2014 Cristie Software Ltd.

Backup Compression and Encryption

The options on this page allow you to setup compression and/or encryption for the backup.

Initially, compression options will be set to **<Use Default>**, which means whatever is set in Encryption Default Settings property pages will be used for this job. If necessary, you can make some adjustments to suit the current job.

Encryption will be enabled/disabled as defined when the script was first created. However, this can be changed using as required.

> ***Note: any changes made here only apply to the current backup selection script and do not alter the Default Settings properties.***

For descriptions of these fields, please refer to the Backup page of the **Default Settings** section in this document for a brief description of the fields.

Script Name

The **Filename** and **Description** entries are optional.

The description entry is what appears in the **Backup Selections** scripts folder, so it makes sense to provide a meaningful description.

The file name is used by the system. The name should comply with the short filename 8.3 convention.

However, if you do not intend to save this script then a name and description are irrelevant.

Media Header Overview

The media header is the overall name given to the media in the Backup Location (or disk file if using a Virtual tape Drive as the Backup Location). Media header information is optional and does not affect how the Backup Selection script performs. If you are saving the script, then meaningful header details should be entered.

Name is a unique identifier for the media loaded in your Backup Location. Ideally the name should reflect the contents of the media. If you need to Restore data, especially in an emergency, headers such as 'Volume 1' and 'Volume 2', without any other description, do not mean anything and will cause a lot of frustration.

Comments field allows you to add more specific details which may be useful in identifying the contents of the tape. It may not be you who is accessing it, perhaps several months from now.

Please take note of the implications of supplying a **Password**. A password will make your data more secure because a Restore operation recognises the password protection and will not proceed until the correct password is entered.

See also the Displaying Media Headers for Backup section in this document.

4.3.1.5 Deleting a Backup Selection Script

To delete a Backup Selection Script, open the **Backup Selections** tool.

Highlight the Backup Selection script you want to remove (single mouse click on the relevant script).

Select Delete from the Backup Selection Scripts top bar menu and press the Delete key.

4.3.1.6 Script Properties

The Backup Selection Script property sheet allows you to define all the details which should apply for this particular backup. You can create as many different backup scripts as you need to cover all backup situations.

4.3.1.7 Running a Backup Using an Existing Selection Script

From the Backup Selections tool you can highlight a script and select **Run** from the **Script** top bar menu

or

Double click on the script to view/modify it and then press the **Backup** button

or

From the CBMR tool, select **Backup Using Existing Script** from the **Tool** top bar menu. This will open the **Backup Selections** tool. Double-clicking on a script will then run it. Once the script has finished, the Backup Selections tool will also close.

When editing a Backup Selection script, the **Estimate** button (which also available from the **Tool** top bar menu) will estimate the size of the backup you have defined: the number of files and the size in Bytes). This could be useful if you need to know in advance how much capacity you require for this backup or estimate how long the job will take to run.

The **Backup Status** window displays a running report on how the backup is progressing. The information is divided into three headings:

Media Details - shows the header information

Current File - details of the file currently being written to the backup

Progress - how many files have been backed up, time taken and so on

4.3.2 Dataset Settings

A dataset is created for each drive that is backed up on the volume. If you do not provide dataset header settings, CBMR will automatically assign a drive letter as the default header.

(In the **CBMR Server Edition**, the default header is the UNC path).

You can password protect a dataset. This provides increased security of data **BUT** make sure you can remember the password. You will be prompted for the password at any future access. There is no bypass procedure and if the password is lost or forgotten, the data will be inaccessible.

When you do a Restore, Compare or Verify, CBMR displays the first dataset. Any remaining ones are listed when you select Next or **All**.

4.3.2.1 Dataset Details

Select the **Settings** button under *Dataset* on the right of the window, the Dataset Info dialogue is displayed. (The **Dataset Info** option in the top bar **Select** window performs the same function.) Notice that the selected drive is identified in the window banner.

Name	Type a name to identify the dataset or accept the default name (drive name)

Copyright © 1998-2014 Cristie Software Ltd.

Comment	The field allows for a brief description of the backup
Password	The data can be made more secure by attaching a password to it. Always choose a password which you can remember easily (see note below)
Save Security Info	You can accept the <Use default>, that is the value defined in Default Settings, or select Yes/No which will apply to the backup script only. If Save Security Info is enabled then all the security details are included in the backup, in addition to the data. This option is only applicable if you have the appropriate user account rights to back up security information

Note: a password is a useful security measure, but you should be aware of the implications. If a backup is password protected, then the password will be requested before the data can be accessed. If you forget the password, there is no bypass procedure and the data will be lost.

4.3.2.2 Estimate Backup Size

The **Estimate Backup Size** option in the **Selections** top bar menu displays a window containing an estimate the size of the backup you have defined (the number of files and the size in Bytes). This could be useful if you need to know in advance how much capacity you require for this backup or estimate how long the job will take to run.

4.3.3 Specifying a Backup Catalogue Entry

Before you create a backup, you need to specify a level of information to be recorded in the catalogue.

There is a *Backup Catalogue* page in the **Default Settings** properties. From here you can specify just how much information you want to store or indeed if you want the backup added to the catalogue.

There are four levels of information (**Brief**, **Partial**, **Full**, **None**). There is a trade-off of space versus level of information. There is no typical setting; which level you use depends on your own requirements. You can change the level at any time if you change your mind about how much information you need to keep.

You can either change the default setting or modify a particular Backup Selection script which will then apply from the next backup or you can modify the Catalogue information level from within the Backup Catalogue window:

Brief	Volume and Dataset headers. This is a minimal level of information and takes up little space
Partial	Volume, Dataset and Directory details
Full	All the above plus File information. This will be significantly larger than Brief or Partial entries
None	Select 'None' if you do not want this particular backup recorded in the catalogue

4.3.4 CBMR Log Files Overview

Log files are a record of completed CBMR operations. You can check the content and determine whether the job was successful. A logfile can be a useful source of information if a problem occurs.

You can request a log file to be created during a Backup, Restore, Compare, Verify and by the Scheduler. The files are named according to the operation (**Backup.log**, **Restore.log** and so on) and stored in the CBMR directory. If a **Backup.log**, **Restore.log** etc. already exists, then logging information is appended to the relevant file for each subsequent operation.

The file can grow rapidly. If you need to retain the information, save it to a new name. (**Save as...** is available from the **File** menu (in Notepad) when you **View** the logfile.) If not, delete it and a new file will be created next time the operation is carried out.

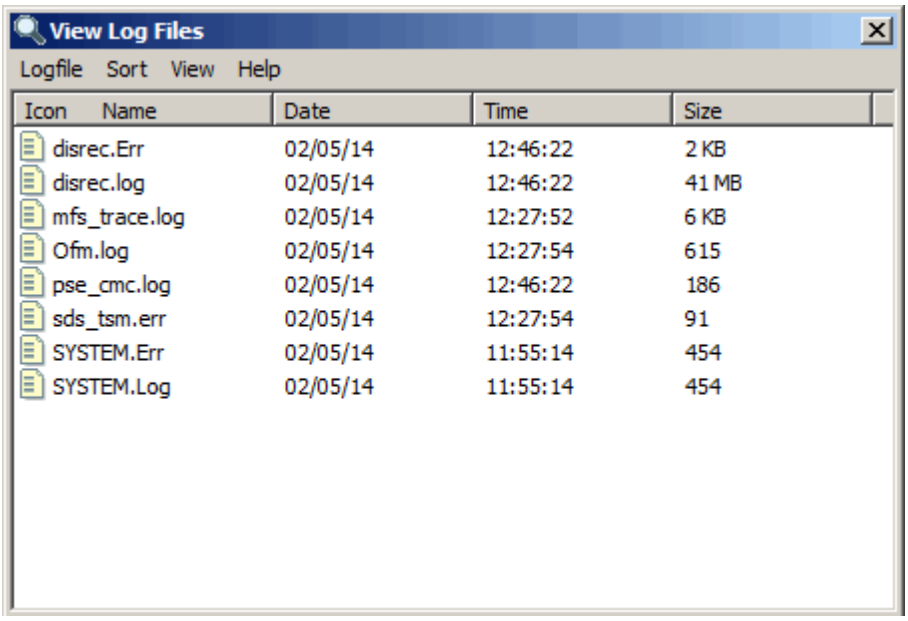
The **View** top bar menu allows you to control the log files display window. The files can be displayed as large/small icons, as a list or as a detailed listing which includes date, time and size details.

The **Sort** top bar menu allows you to sort the files in alphabetic sequence (**Sort by Name**), in date (**Sort by Date**) or in size sequence (**Sort by Size**).

> *Note: in the Details view you can click in the relevant column heading to sort the display in the Name, Size or Date/Time sequence.*

4.3.4.1 Managing Log Files

The **View Log Files** main menu option allows you to control the log files display window. The files can be displayed as large or small icons, a list or as a detailed listing which includes date, time and size details as shown in a sample screen below:


View Log Files
Logfile Sort View Help
Icon Name Date Time Size
disrec.Err 02/05/14 12:46:22 2 KB
disrec.log 02/05/14 12:46:22 41 MB
mfs_trace.log 02/05/14 12:27:52 6 KB
Ofm.log 02/05/14 12:27:54 615
pse_cmc.log 02/05/14 12:46:22 186
sds_tsm.err 02/05/14 12:27:54 91
SYSTEM.Err 02/05/14 11:55:14 454
SYSTEM.Log 02/05/14 11:55:14 454

The **Sort** top bar menu options sorts the files in alphabetic sequence (**Sort by Name**), in date (**Sort by Date**) or in size sequence (**Sort by Size**).

> *Note: if the Details view is displayed, you can also sort the entries in Name, Date, Time or Size sequence by clicking in the relevant column heading.*

Default Settings

Log Files are controlled from the Default Settings. Select the **Default settings...** option from the **Logfile** top bar menu. This takes you directly to the log file property page. You can request:

Copyright © 1998-2014 Cristie Software Ltd.

Full	Contains a complete file listing, errors (if any) and statistics
Partial	Contains only errors and statistics
None	No log file is created

The default log file settings can be overridden by changing the *Logfile Settings* from within a Backup Selection script's Backup Options page.

4.3.4.2 Viewing and Deleting Log Files

Viewing Log Files

To view a Log File, highlight the relevant logfile in the Log Files window and select **View Logfile** from the **Logfile** top bar menu

or

double click on the required logfile.

The logfile will be opened using the Windows Notepad application. If you require a printed copy of the file, select the **Print File...** option from the **File** menu (in Notepad).

Deleting Log Files

To delete a logfile,open the Logfiles tool and highlight the relevant logfile (single mouse click).

Then select Delete from the **Logfile** top bar menu. You are then prompted to confirm the Delete action.

4.3.5 Backup Encryption

CBMR supports backup encryption. This section describes how encryption is handled and some important encryption key management concepts.

4.3.5.1 The Key Repository File

This file is central to the normal operation of encryption in CBMR. It is created when CBMR first starts (if not already present) and contains three major parts:

1. The first part is identified by a single entry named **[Main]** and contains the currently defined default key. A default key is created at random when CBMR first creates the Key Repository file.

2. The second part stores the currently available User defined keys. These keys are created during the definition of a backup script, so this section is a placeholder for the key. They are identified by entries like **[REF.ScriptName]** where *ScriptName* is the user defined name of the script.

3. The final section contains a history of keys used for all encrypted backups made since CBMR was installed. This includes both disaster recovery and non disaster recovery backups. They are identified by entries of the form **[VOL.MediaID]** where *MediaID* is a unique reference created when the backup is made and stored in the volume header of the backup media.

The file is normally created in the CBMR installation folder by default, but may be re-directed to another location via an entry `KeyRepository = <New directory>` in the section `[File Locations]` of the cbm.ini file (itself located in the CBMR installation folder). In this way the file could be located on a network share or a local USB disk for example.

One of the major benefits of this file is that during a backup restore operation, there is no need for a user to remember what key or passphrase was used for a particular backup. If a non-DR backup is being restored, the Key Repository file will normally be directly available on the local system (unless relocated offline) and there is no need to prompt for the passphrase or key. If restoring a DR backup, then the Key Repository file can be supplied via a network share or a USB key for example. If the file is not available or no matching backup entry is found, only then will CBMR need to prompt for the passphrase or key.

4.3.5.2 Passphrases and Encryption Keys

The **Encryption Key** used for a particular encrypted backup can be supplied in one of three ways:

Default key - use the system-wide defined key

User supplied key - the key used will be supplied by the user prior to the backup

Dynamic key - use a randomly generated key

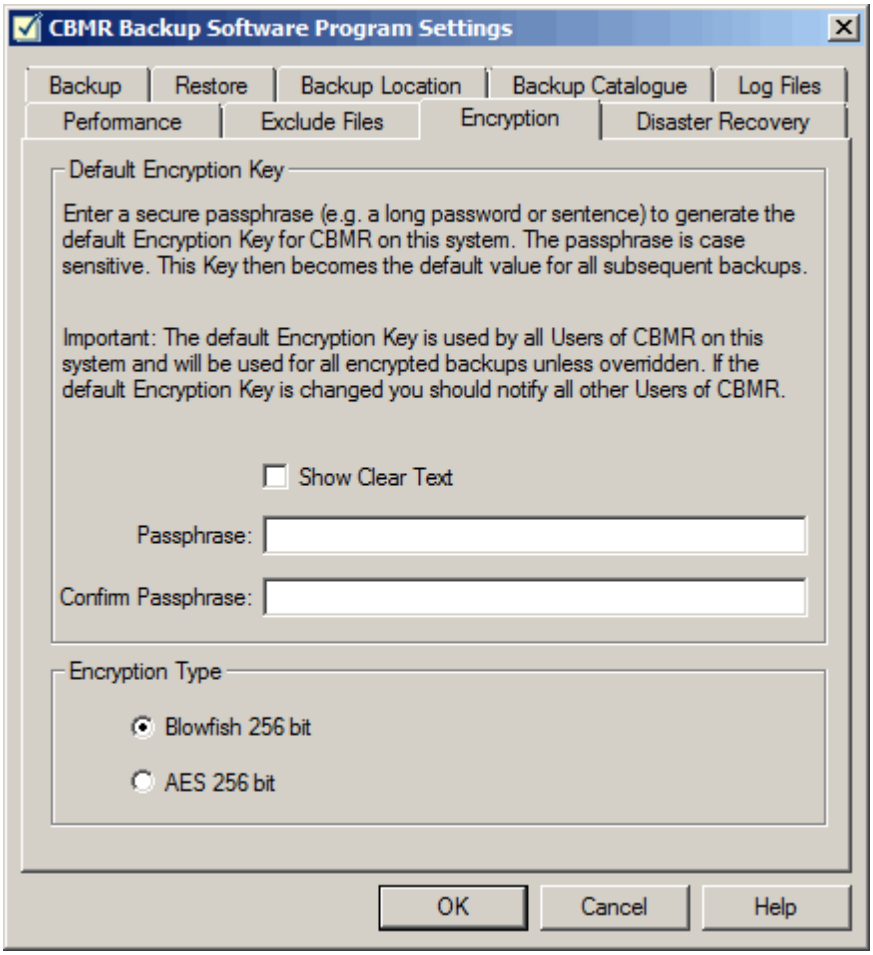
A **passphrase** is a user-friendly form of an encryption key. CBMR uses the passphrase to generate an **Encryption Key**. The passphrase itself is never stored or used directly - only the resulting key. For example,it is much easier to remember the phrase `"mary had a little lamb"` than the key `"QBN3EHYD-JNF3JQRB-MLJR9YV4-UFPQLHA5-JEYKVWTH-7PCA8XW7-8FVMJTKD"`.

> ***Note: passphrases are case sensitive. They should be made secure, eg a long sentence or a long password. The minimum length is one character.***

The Default Encryption Key

The default encryption key can be overridden at any time by selecting the Encryption tab on the Default Settings menu option:

Copyright © 1998-2014 Cristie Software Ltd.


CBMR Backup Software Program Settings
Backup
Restore
Backup Location
Backup Catalogue
Log Files
Performance
Exclude Files
Encryption
Disaster Recovery
Default Encryption Key
Enter a secure passphrase (e.g. a long password or sentence) to generate the default Encryption Key for CBMR on this system. The passphrase is case sensitive. This Key then becomes the default value for all subsequent backups.
Important: The default Encryption Key is used by all Users of CBMR on this system and will be used for all encrypted backups unless overridden. If the default Encryption Key is changed you should notify all other Users of CBMR.
Show Clear Text
Passphrase:
Confirm Passphrase:
Encryption Type
Blowfish 256 bit
AES 256 bit
OK
Cancel
Help

This value will then be used for all subsequent encrypted backups where the default Key is selected. If this default is changed, it is important to notify all other users that it has been changed.

4.3.5.3 Restoring Encrypted Backups

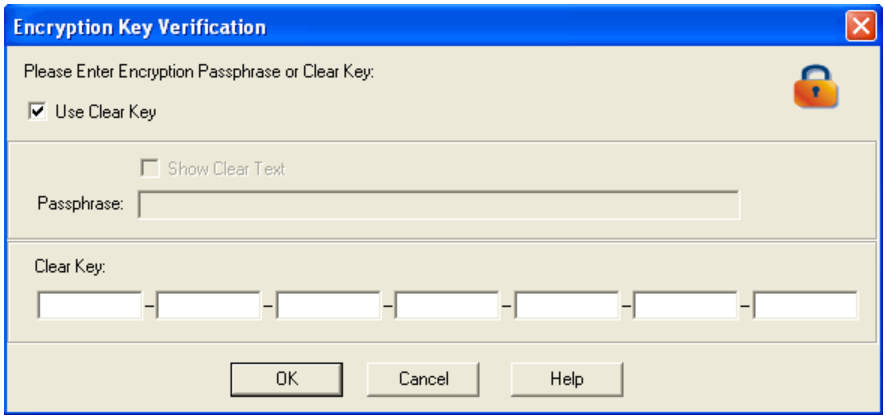
In general, restoring encrypted data either requires access to the **Key Repository** file or a manually entered passphrase or key.

When restoring an encrypted backup, CBMR will use the following sequence to obtain the correct encryption key:

- The Key Repository file is searched to find a matching entry for the MediaID (obtained from the media Volume header of the backup). If a matching entry is found, the key is extracted and the backup restored with no user interaction

  Note: if the key specified in the matching entry is found to be incorrect, processing continues at the next step

- If no matching entry is found for MediaID or an incorrect key is found, then a check is made using the current default key. If the key is correct, the backup is restored with no user interaction
- If the default key is also incorrect, then the user is prompted for the passphrase or key:



- Enter the key or un-tick the **Use Clear Key** tick-box and enter the passphrase instead

During an encrypted DR backup restore, the user will be prompted for the location of the **Key Repository** file, since it will not necessarily be located on the local system.

4.3.5.4 Encryption Algorithms

Two encryption algorithms are available - **Blowfish 256-bit** and **AES 256-bit**. Blowfish is typically faster to encrypt than AES. Beware, however, that enabling encryption significantly slows down the backup.

> *Note: the Blowfish algorithm is sourced from Bruce Schneier (www.schneier.com/blowfish.html)*

4.3.6 Start Backup

When you have defined the Backup Selection script, you can run it immediately by selecting the **Backup** button.

The Backup Status window keeps you informed about how the backup is progressing.

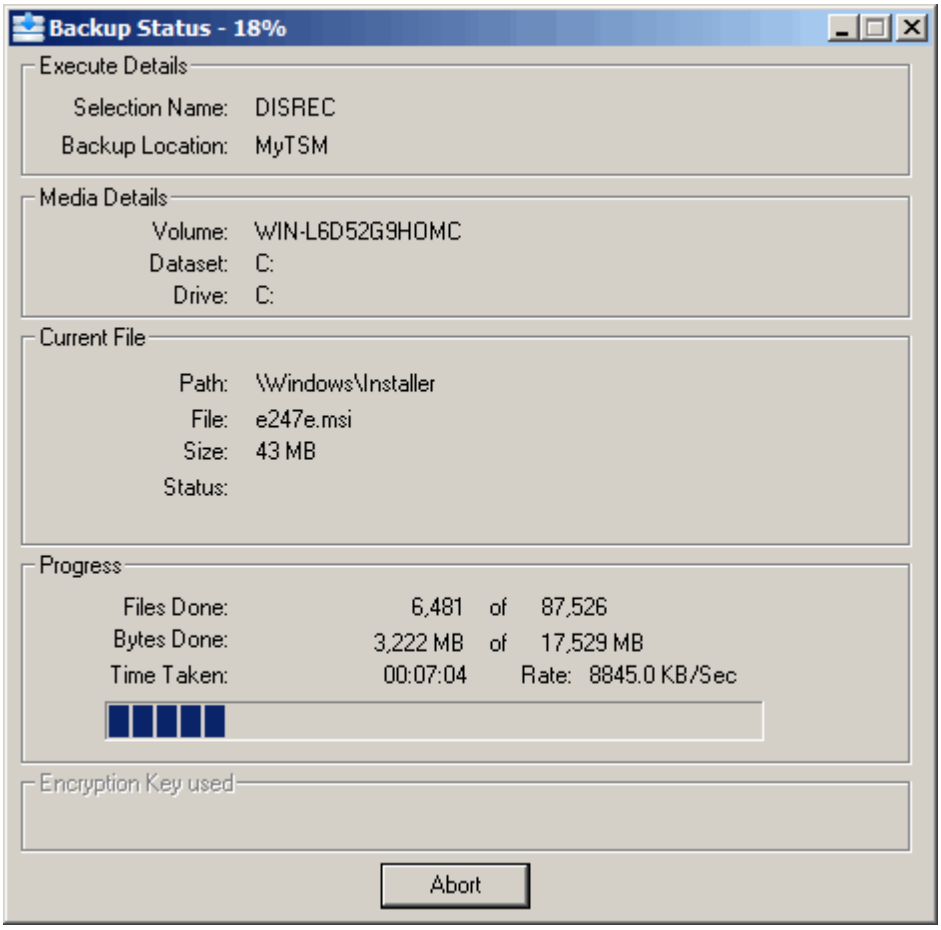
You will get a format warning message if the loaded tape has been recorded in a different format from CBMR. You are prompted to overwrite the tape via a Yes/No? prompt.

Select 'No' and the backup is aborted; select 'Yes' and the tape will be treated as a new piece of media (a new media header is created and existing data overwritten).

> *Note: there is an Estimate Backup Size option in the Selections top bar menu which will detail the size of the backup you have defined. This could be useful if you need to know in advance how much capacity you require for this backup.*

While a Backup (Restore, Compare or Verify) is running, a status window is displayed:

Copyright © 1998-2014 Cristie Software Ltd.



This displays:

Execute Details - volume dataset name being recovered and the Backup Location name

Media Details - shows the header information: Volume, Dataset and Drive

Current File - details of the file currently being written to the backup

Progress - a running count of files backed up, bytes done, time taken and backup rate

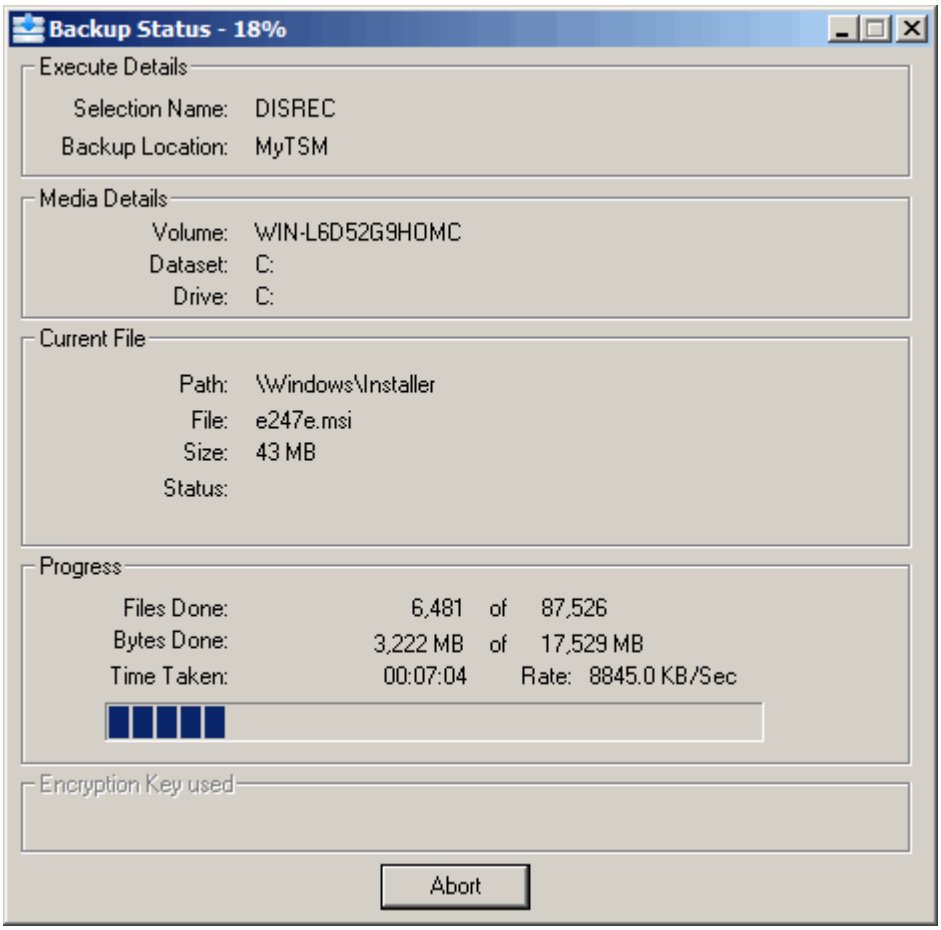
When the job is complete, a statistics window is displayed which gives you an immediate report on the job.

The **Detach** button only appears on the Backup Status screen if the job has been initiated from the scheduler. Pressing the **Detach** button causes the job to run as a background process with no user console interaction.

If you want to attach to a job which is running in detached mode: run CBMR, open the **CBMR Backup Schedules** tool, select the 'running job' and select **Attach** from the **Jobs** top bar menu (or double click the 'running' job) to open the Backup Status window.

4.3.7 Aborting Backup

If you need to stop the backup, there is an **Abort** option in the CBMR Backup Status window (the window displayed when the backup starts running) which allows you to stop the operation.



However, CBMR begins to process the first command it receives, which is **Start**, before it receives and can process the **Abort** command. As as a result, the header details are written before the operation stops. If the backup selections script requests overwrite rather than append, then existing data will be overwritten.

4.3.8 Verify and Compare

Restore, Verify and **Compare** are related functions which use a common interface. These commands are accessible from the **Tools** drop-down menu.

Verify and/or **Compare** should be run after every backup to make sure that the tape is in good condition, the read/write heads are clean and the data has been reliably recorded.

Verify checks that the data can be read back from tape, it will not check the data for accuracy.

Compare checks for data accuracy. The program performs a byte by byte comparison of the backed up data on the tape with the source data on disk. For this reason it will take considerably longer to complete than a Verify.

You are recommended to run both programs when you use CBMR for the first time, to ensure that the software and the Backup Location storage devices are working correctly.

Verify

It is good sense to verify your data after a backup to ensure that it can be restored. **Verify** checks

Copyright © 1998-2014 Cristie Software Ltd.

the data for readability; it does **not** guarantee its accuracy.

Verify should be run after every backup to make sure that the tape is in good condition and the read/write heads are clean.

You are recommended to run **Verify**:

1. When you first use CBMR to do a backup, to ensure that the software and the Backup Locations are all working correctly
2. Periodically to ensure the continued accuracy of your backups

Compare

Compare is different from **Verify** in that it performs a byte by byte comparison of the backed up data on the tape with the source data. For this reason, it will take considerably longer to complete.

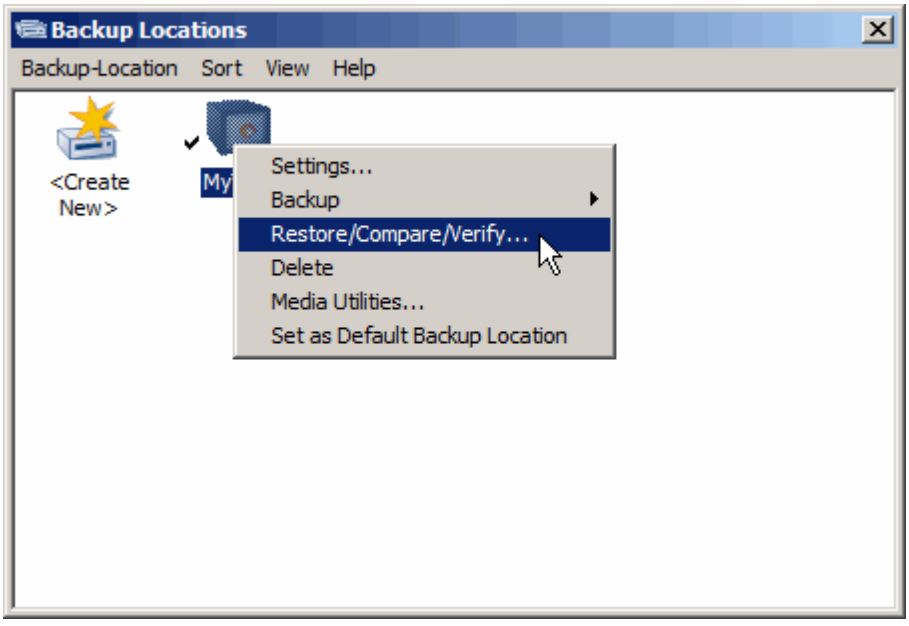
You are recommended to run **Compare**:

1. When you first use CBMR to do a backup, to ensure that the software and the Backup Locations are all working correctly
2. Periodically to ensure the continued accuracy of your backups

4.3.8.1 Programs

The **Restore, Verify** and **Compare** programs can be run from the CBMR Tools drop-down menu (click the Restore, Verify or Compare icon)

or from the Locations top bar menu in the Configuration *Backup Locations* option:



If running from the drop-down Tools menu, the first step is to choose whether to access the data via the **Backup Catalogue** or directly via the **Backup Location**.

If you are checking the backup immediately after it has completed, then you will probably access the data via the Backup Location. If you want to check an earlier backup and you are not sure where the data is located, then using the Backup Catalogue is the quickest option.

4.3.8.2 Dialogue

The Compare and Verify programs each present a similar screen display. The window opens with the top level tape icon and first dataset displayed. The other screen features are described below:

The **Scan** options are used to scan the tape and display each dataset in turn. Each time you click on the Next button, the next dataset on the tape is displayed until no more datasets are found. Alternatively, you can display the complete structure in one step by selecting **All**.

You can confirm the tape that is loaded by checking the **Media Header** details. Highlight the top level (root) tape icon and select the Show Details... button. Similarly, pressing the Show Details... button when a dataset is selected will display the **Dataset Header** details.

You can also display Header details by double clicking on the root icon (Media Header) or individual datasets (Dataset Header).

Tag or untag files and directories as required.

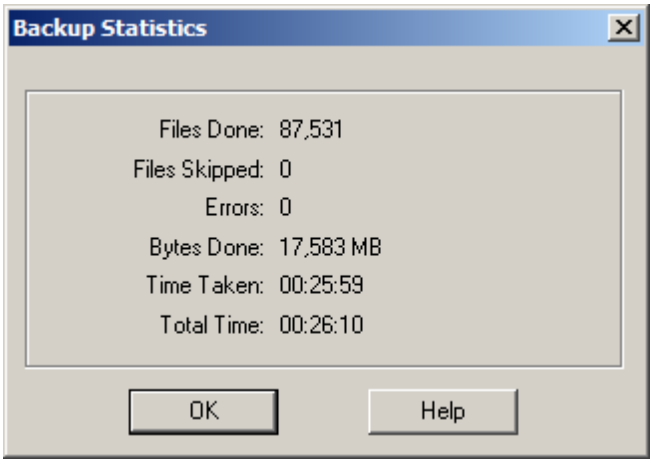
To begin a Restore, Verify or Compare operation, click the appropriate button at the top of the window.

CBMR displays a progress report and will warn you if any problems occur. The window title reflects which program is running (*Restore, Compare Status* or *Verify Status*).

A **Statistics** window is displayed when the job is completed. This information is written to the relevant log file (**restore.log, compare.log** or **verify.log**) if one has been requested.

Redirecting files has no purpose in a VERIFY or COMPARE job.

4.3.9 Statistics Report



When a backup job is completed, a **Statistics** window is displayed which gives you an immediate report on how many files have been backed up, skipped, errors encountered (if any) and so on.

These statistics will be written to the relevant log file (provided a log file has been requested in the Default Settings). For example, **backup.log** for a Backup job, **restore.log** for a Restore job).

4.4 Restoring Files

Maintaining an efficient backup routine is useless unless the data can be restored correctly. A restore routine for day to day files, plus for disaster recovery situations, is just as important as a backup routine. You are recommended to run practice restores to a spare drive to ensure that you are confident using the Restore program **BEFORE** you need to do it in a 'real' situation.

Copyright © 1998-2014 Cristie Software Ltd.

Also it is good sense to run restores periodically to check that data is being correctly restored without errors. It is possible for hardware errors to occur which are not immediately obvious but which may corrupt the data.

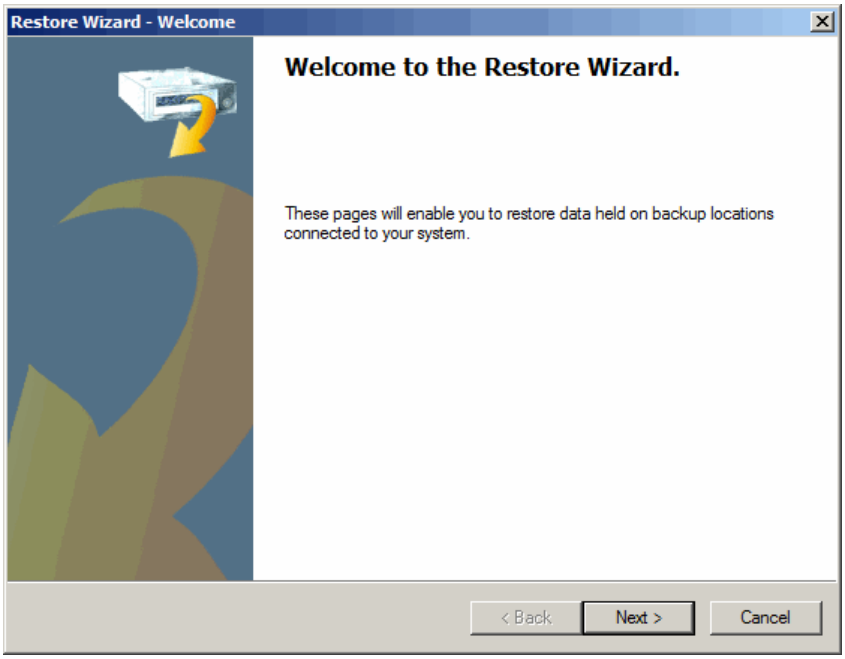
Restoring data means that files are written from the backup media to the disk.

There are a number of ways of restoring files:

- The **Restore Wizard** can be run by selecting **Restore** from the **Tools** menu. This will guide you through the restore process
- The media in a specific **Backup Location** can be browsed by highlighting it in the **Backup Locations Tool** and selecting **Restore / Compare / Verify**. Data can then be selected and restored
- A Backup Catalogue **Volume** can be browsed by highlighting it in the **Backup Catalogue Tool** and selecting **Open** from the top menu bar

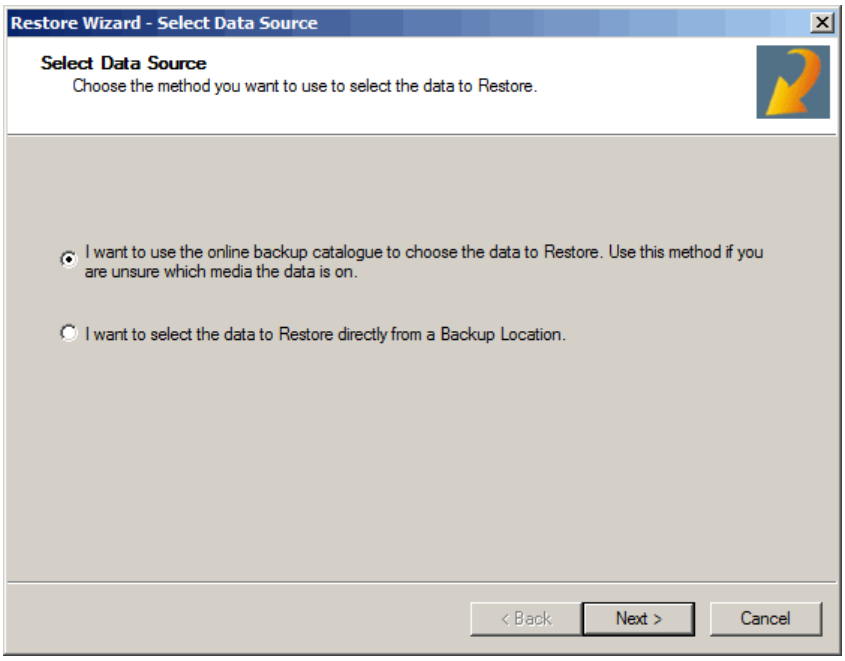
4.4.1 Restore/Compare/Verify Wizard

Separate **Restore, Compare** and **Verify Wizards** are provided. However they are very similar and so the help is presented using the **Restore Wizard** as an example:


Restore Wizard - Welcome
Welcome to the Restore Wizard.
These pages will enable you to restore data held on backup locations connected to your system.
< Back
Next >
Cancel

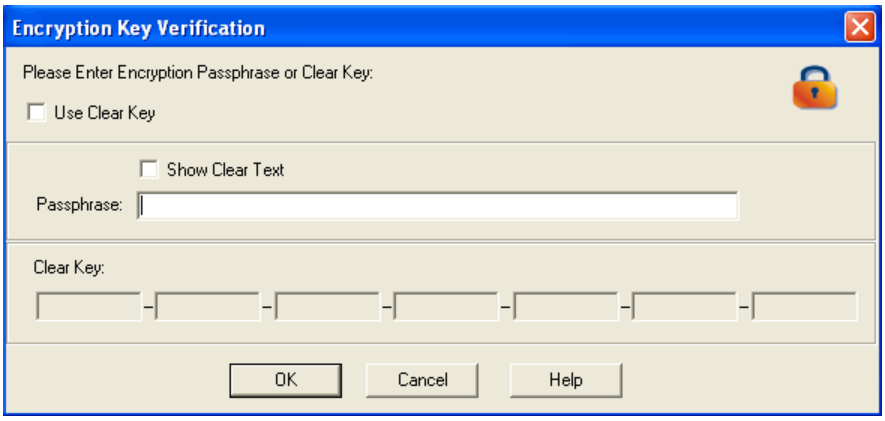
This wizard is displayed when you select Restore, Compare or Verify from the **Tools** menu. The options are the same in all three cases, but the action performed at the end of the wizard differs. You have an opportunity on the final page to cancel or change the action requested.

4.4.1.1 Data Source


Restore Wizard - Select Data Source
Select Data Source
Choose the method you want to use to select the data to Restore.
I want to use the online backup catalogue to choose the data to Restore. Use this method if you are unsure which media the data is on.
I want to select the data to Restore directly from a Backup Location.
< Back
Next >
Cancel

On this page, you choose whether to use the Backup Catalogue or the media currently in the default Backup Location to select the data to restore, compare or verify.

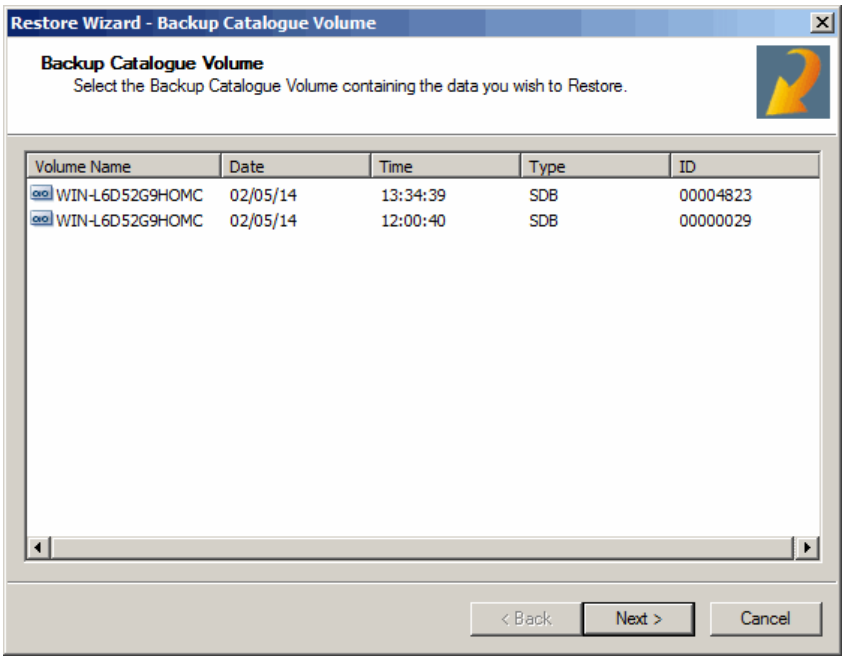
If the backup is encrypted and you choose *'I want to select the data to Restore directly from the media in the default backup location'* and then press Next>, you may see the following dialogue:



This will only be displayed if a Key entry for the backup is **not** found in the Key Repository file. In this case, enter the required passphrase or Key to recover the backup.

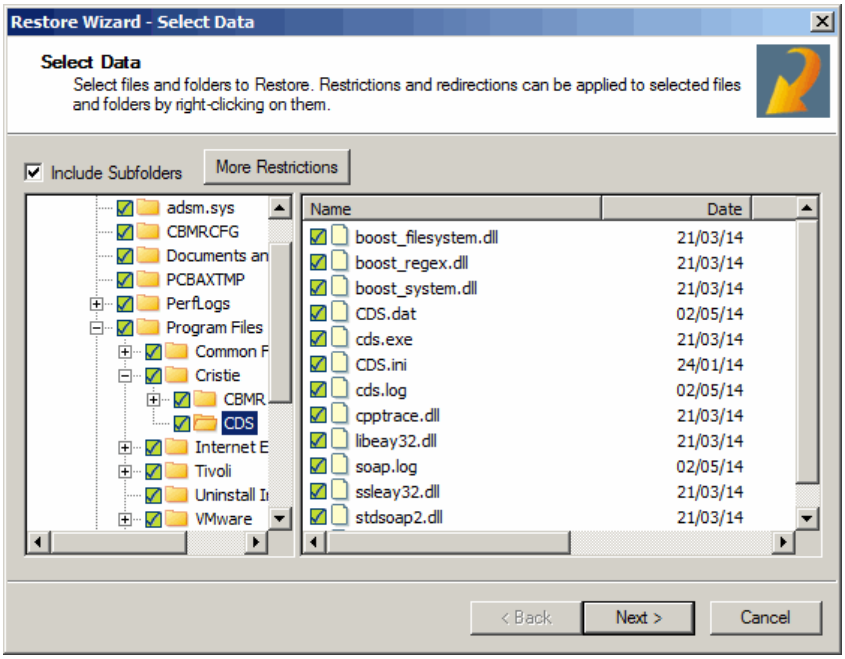
Copyright © 1998-2014 Cristie Software Ltd.

4.4.1.2 Catalogue Volume



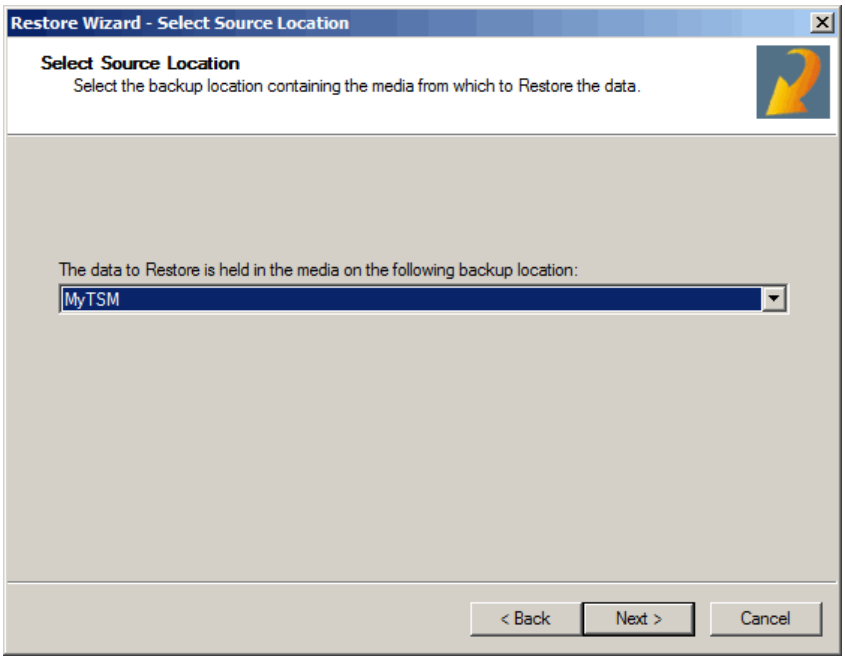
This screen will only appear if you have opted to use the **Backup Catalogue** to select the data. Here, you select the Backup Catalogue volume that lists the data you wish to restore, compare or verify.

4.4.1.3 Select Data



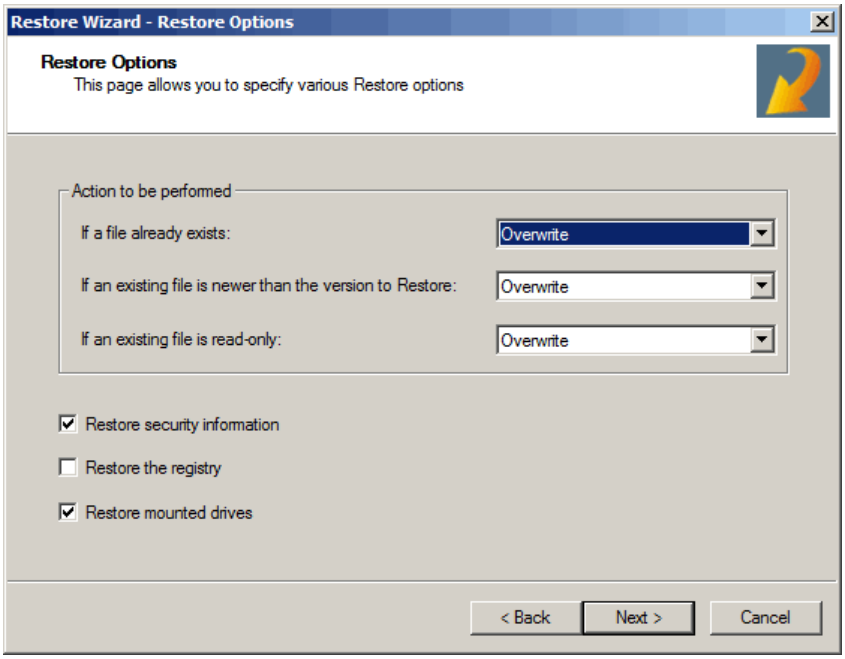
This screen allows you to actually select the data you wish to restore, compare or verify. If you are selecting your data directly from the media in the default Backup Location rather than from the Backup Catalogue, then browsing the data can involve delays as the media is read.

4.4.1.4 Select Location


Restore Wizard - Select Source Location
Select Source Location
Select the backup location containing the media from which to Restore the data.
The data to Restore is held in the media on the following backup location:
MyTSM
< Back
Next >
Cancel

This screen will only appear if you have used the **Restore directly from a Backup Location** to select the data to restore, compare or verify. Here you select the **Backup Location** on which the required media is loaded.

4.4.1.5 Restore Options



This page allows you to set various options regarding the data to restore. The options set here are only applicable to restore operations and have no effect on compare or verify operations.

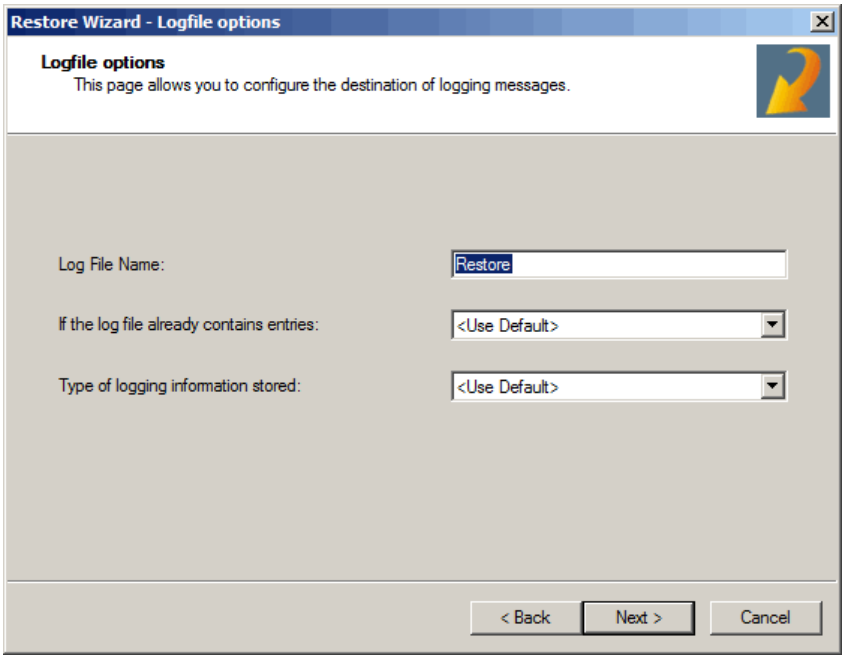
(Windows NT Only) Select the **Restore Security Information** option if you want to restore the security information associated with the directory. If the option is not ticked, then only the data is included.

> *Note: you must be logged on the computer as a user account with the appropriate rights to restore security data.*

Copyright © 1998-2014 Cristie Software Ltd.

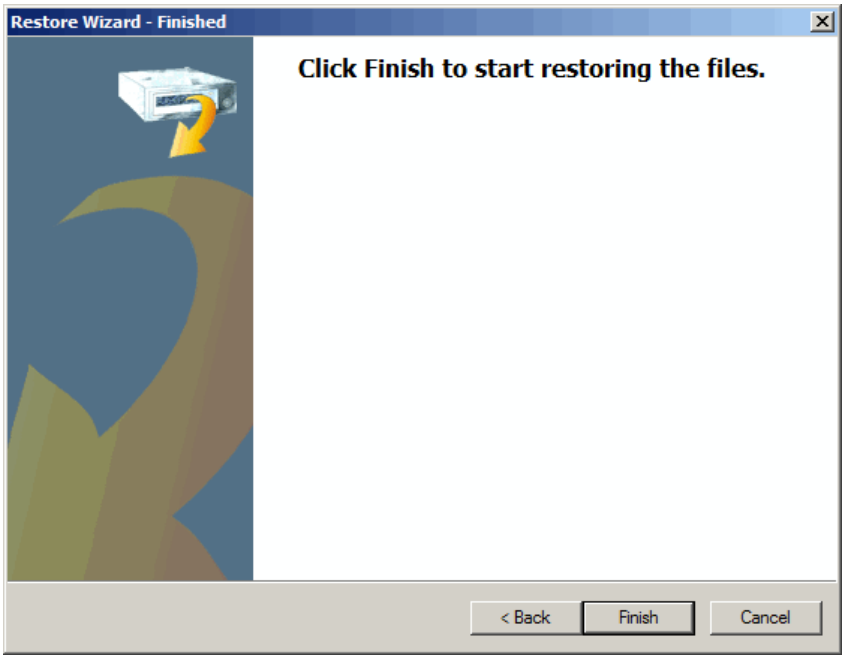
Select the Restore the Registry option if you want to restore the **Registry** files. You must reboot your system after restoring the registry files.

4.4.1.6 Logfile Options



This page allows you to set the amount of logging information saved and the file it is saved in.

4.4.1.7 Finished



This page is displayed once all the restore, compare or verify options have been set. You have the option on this page to change your original decision on which action should be performed. Pressing Finish will initiate the chosen action.

4.4.2 Restoring From the Backup Catalogue

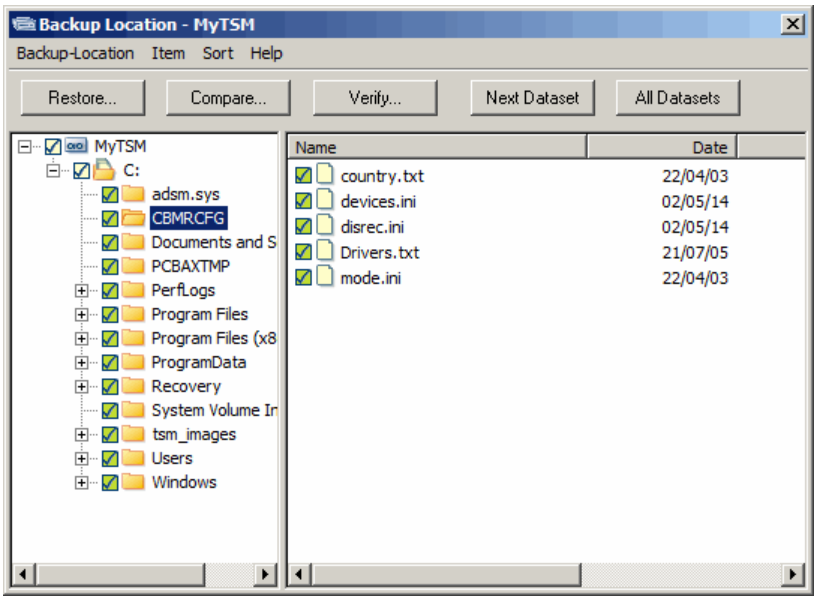
If you click on **Use Backup Catalogue**, then the screen displays a listing of the Backup Catalogue contents.

Use the Backup Catalogue options to view the catalogue information and make your selection.

Before the operation takes place, CBMR checks the Backup Location and the Media Header selected from the Catalogue against the connected location and the loaded media. If either items conflict, then an error message is displayed and you are prompted to correct the situation.

For further details, please refer to the section on Restoring Registry Files.

4.4.3 Browse Backup Location



The **Backup Location** browse screen will appear when you select **Restore/Compare/Verify** on a Backup Location. You are able to select data to process directly from the media in the specified location.

> ***Note: operations available on this screen can take some time as the media will need to be read.***

Buttons are provided to begin a restore, compare or verify operation, and also to read the next dataset and all datasets on the media.

The Locations menu provides options to set **Restrictions** on whether the selected data is actually restored, compared or verified, to change Backup Location **Default Settings** and to **Close** the location.

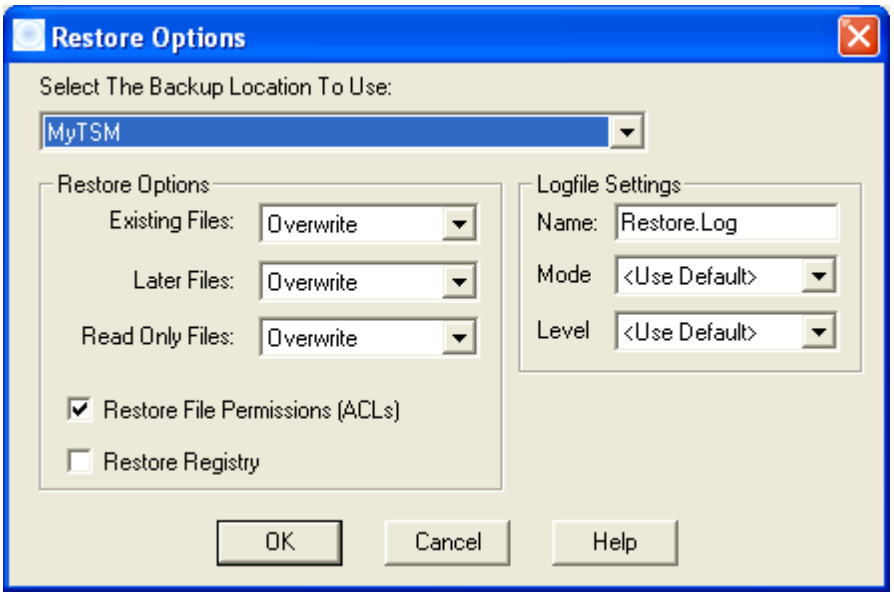
The Item menu (which is also available as a context menu) provides options to **Tag** or **Untag** the selected item, view the **Dataset Header** for the selected dataset, view a **Selection List** of the items selected from the current dataset, **Redirect** an item to a different location from where it was originally backed up, view a **Redirection List**, and view the **Media Header** for the media in the Backup Location.

The **Sort** menu is available when at least one item is highlighted in the file list view. It enables the file list to be sorted in a variety of ways. The file list can also be sorted by clicking on the list's column headers.

For reference, see also the Media Header and Dataset Header for Backup Catalogues chapters in this document.

Copyright © 1998-2014 Cristie Software Ltd.

4.4.3.1 Options (Restore/Compare/Verify)



The title of this window depends on which program you have selected: Restore, Compare or Verify. However, you are not bound by that selection and if you change your mind, for example you decide to compare the data before you restore it, then you can run the Compare program from this window.

You can accept the default settings or you can specify different rules which will only apply to the current job.

> *Note: any changes made here will not change the values defined in the Default Settings property sheet.*

Select the backup location to use

Select the location from which you are accessing the data. All the configured locations are listed.

Restore Options

- **Existing Files** - if any files being restored already exist on disk then you can direct CBMR to respond in one of the following ways:

- *Skip* any file it encounters which already exists

- *Ask* whether it should overwrite or skip the file

- *Overwrite* the existing file with the file from the backup

- **Later Files** - if any files being restored are found to be later versions than those already existing on disk, then you can direct CBMR to respond in one of the following ways:

- *Skip* any file it encounters which are later versions

- *Ask* whether it should overwrite or skip the file

- *Overwrite* the file on disk with the later version from the backup

- **Read Only Files** - if any read only files are being restored already exist on disk, then you can direct CBMR to respond in one of the following ways:

- *Skip* any read file it encounters which already exists on disk

- *Ask* whether it should overwrite or skip the file

- *Overwrite* the file on disk with the file from the backup

Logfile Settings

Log files are a useful source of information and will list any error messages. Log file information can be important if problems have occurred. The following options are available:

- **Name**

- the default will be the log file of the selected operation (restore.log, compare.log or verify.log). If you have decided to run a different program from the one selected in the Tools menu, for example Compare instead of Restore, then you will have to overtype the default entry with the log file name relevant to the operation

- **Mode - Overwrite/Append**

- if *Overwrite* is set, then each time the log file is created it overwrites the existing one

- if *Append* is set, then each log file is appended to the previous one

- **Info Level - Full/Partial/Brief/None**

- a *Full* logfile contains a list of all files, errors (if any) and statistics

- a *Partial* log file contains sub-directories, errors (if any) and statistics

- a *Brief* log file contains errors (if any) and statistics

- if *None* is selected, then no log file is created

Restore Security Info - (Windows NT installations only)

Select this option (ticked) if you want to restore the security information associated with the directory. If the option is not ticked, then only the data is included

> ***Note: you must be logged on the computer as a user account with the appropriate rights to restore security data***

Restore Registry

Select this option if you want to restore the Registry files. You must reboot your system after restoring the registry files.

4.4.4 Redirecting Files

The **Redirect** window allows you to restore your files to a location different from the source. All you need to do is select the relevant directory, select the **Redirect** option and the re-direction dialogue is displayed.

> ***Note: redirecting does not apply to the Compare or Verify operations.***

4.4.4.1 Redirection Dialogue

The Redirection Dialogue shows the Source Directory (the path is already entered). Type the destination path (the disk and directory where you want the files restored to). For example, you could request that all tagged files are restored to **c:\temp**.

If you want to view which directories have been redirected and their destinations, then select the **Redirection List...** option from the **Item** top bar menu.

You can direct other files (**Add**), change the destination (**Modify**) or remove an entry (**Delete**).

Copyright © 1998-2014 Cristie Software Ltd.

Once you have instructed Restore what to restore and where to restore it to, press the Restore button.

It is possible to compare restored files. Please note that if they have been redirected to a different location from their source, then the path you enter for the compare must **exactly** match the redirected path.

4.4.4.2 Redirection List

The Redirection List shows all the redirections defined for the current dataset. You can add to the list, modify it or delete entries.

Once you have instructed Restore what to restore and where, press the **Restore** button.

4.5 Windows Registry

The Registry is a hierarchical structured collection of settings that control the operation of virtually all of the components within a Windows system. This includes the operating system, applications and user preferences.

It is very important that you make regular backups of the registry and understand how to restore it should a disaster occur.

Important notes:

1. To backup or restore the registry you must be logged on to the system as a user with *Administrator Rights*

2. After restoring the registry, there are some files in the **\pcbax\temp** directory on the system drive which will be locked and cannot be deleted. However, after the system is rebooted the registry replacement takes effect and these files can be deleted. It is now safe to delete all the files in the **\pcbax\temp** directory

3. If you do not specify the **Restore Registry** option, then none of the active registry files will be restored and a 'File is locked' warning will be issued for each file. Enabling the Restore Registry option informs CBMR to replace the existing registry files and causes it to perform special processing on these files

4. A full backup of the system drive will also contain the registry files (assuming the user had sufficient *Rights* for this). The important point here is that if you wish to restore an entire system drive but do not want the registry to be restored, then this is possible by tagging all files but **not** selecting the **Restore Registry** option. Likewise, if you **do** want all files and the registry restored, tag all files and select the **Restore Registry** option - there is no need to restore the registry dataset separately

5. The dataset containing the registry files is a standard dataset containing ordinary file images. The registry is not backed up as any special data type. This is done to facilitate disaster recovery operations and also to allow advanced users to be able to restore individual user profiles

4.5.1 Structure of the Registry

The registry is composed of many files and the names of these are dependent on the version of operating system that is running.

Most of the files are normally located within the **system32\config** directory below the main Windows System directory.

User Profiles

User profiles are automatically mapped to the registry when a user logs on to the system. At this point, the file(s) that hold the user profile information are locked and become unavailable for normal file backup. Active user profiles can only be accessed using the registry API functions.

4.5.2 How is it backed up?

CBMR provides the user with a simple and easy-to-use method of backing up the registry files by showing the registry as a separate resource that can be selected along with the available drives.

If this resource is selected, a separate dataset will be created containing all of the files that comprise the registry. In addition, all user profiles are backed up into this dataset - this includes both active and inactive profiles.

4.5.3 Restoring

Restoring the registry needs to be given careful consideration because any changes that have been made since the registry was backed up will be lost. For example, any application installed since the backup will no longer be known to the system.

If it is necessary to restore a registry, for example due to a registry corruption, the following steps should be taken:

1. Tag all files in the registry dataset containing the most recent copy of the registry
2. Ensure that the **Restore Registry** option is checked in the Restore Options dialogue (Restore Options button in the Restore window)
3. Start the Restore
4. When the restore has completed, the system **MUST** be rebooted to enable the registry change to take effect

The reason for having a Restore Registry option that must be used in addition to selecting the data, is to force a separate and specific request to restore the registry. This prevents an accidental restore which is an irreversible process that may have severe consequences.

4.6 Scheduler Overview

The **CBMR Scheduled Jobs** tool allows you to set up jobs to run automatically and is a trouble free way of maintaining your Backup regime. Once you have defined the jobs (...what needs to be backed up and when) and added them to the jobs list, the scheduler will simply carry on and do the work without further intervention from you.

The CBMR Scheduled Jobs tool does not require any complex command statements; the property pages provide an easy to use interface enabling you to create new jobs and add them to the jobs list, update jobs or remove out-of-date jobs.

CBMR uses the standard Task Scheduler service provided with Windows.

This provides flexible schedules to be set up (for instance 'every 10 minutes from 09:00 for 1 hour every Mon, Wed of every 2 weeks'). You can easily maintain a daily, weekly and monthly backup routine by creating a job for each backup and adding it to the schedule list.

Copyright © 1998-2014 Cristie Software Ltd.

You can use the same Backup Selection script or command file for several jobs, but each must have different time/date parameters. CBMR will not allow two jobs of the same specification to be created.

For additional information, please also see the System Dependent section for Schedulers in this document.

4.6.1 Operating the Scheduler

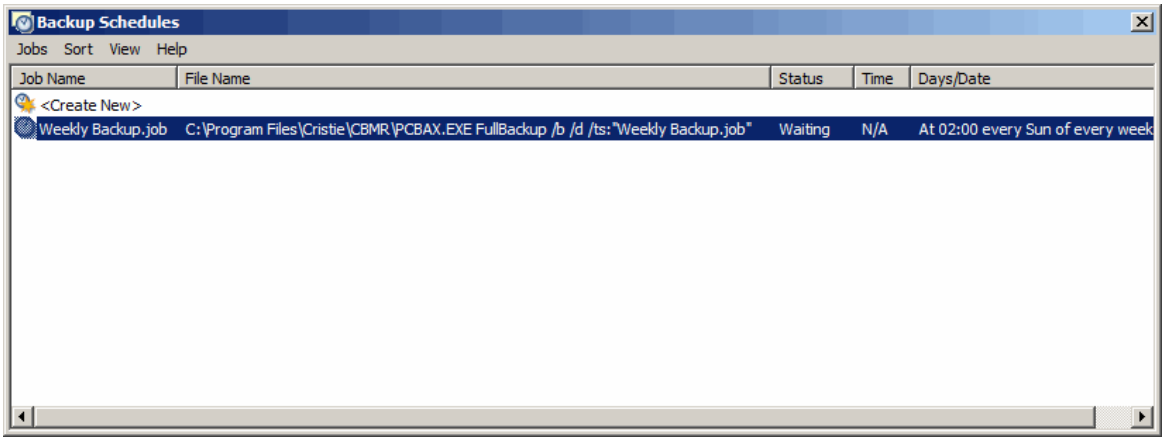
The Scheduler tool is accessed by selecting the **Backup Schedules** option from the **Configuration** menu

The **CBMR Scheduler** tool allows you to manage scheduled jobs. Jobs are serviced by the *Windows Task Scheduler service*.

The top bar **Jobs** menu contains all the scheduler related tasks such as creating a job, modifying an existing job, putting a job on hold and attaching to a scheduled job.

Similar to other windows, you can **Sort** the job list and change the **View** (large/small icons, a list or details). The **Details** view allows you to monitor the state of jobs. It shows you the most information about a job (status, run time and the Days/Date).

The icon representation will identify the status of a job. For example, a scheduled job will have a plain clock icon, a running job will have a tick superimposed on the clock and a job requiring user intervention will have a warning symbol superimposed.



The Schedule dialogue contains all the fields required to define a job to be scheduled to run at a particular time. This window may contain an existing schedule with all the fields defined, or if you have selected the <Create New Job> icon (or the **Create New** option in the **Jobs** menu/context menu), the fields will be blank.

The Schedule dialogue contains a property sheet with three pages. The first page details the job that will be run, the second page details the times that the job will be run and the third page details various advanced settings, such as how long the job will be allowed to run.

4.6.2 Creating a New Scheduled Job

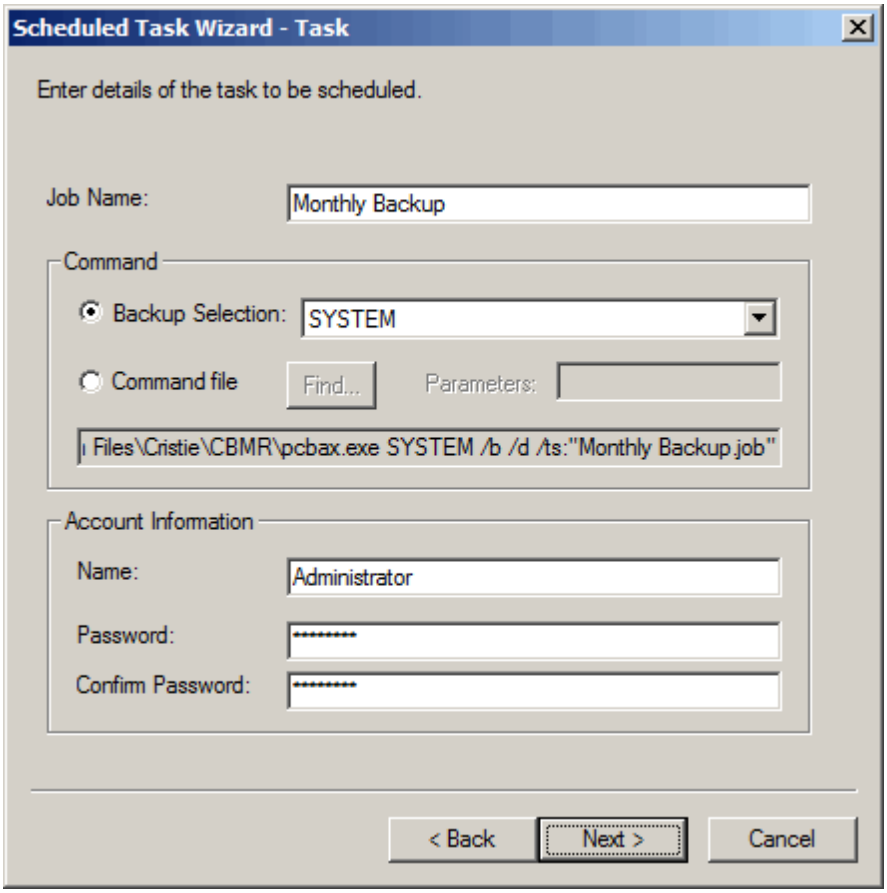
To create a new Scheduled Job, click on Run or select the **Schedule Disaster Recovery** option on the main menu. You can also select **Backup Schedules** from the **Configuration** dropdown menu.

Then double click on the *'Create New Job'* icon in the Scheduler tool or **New Job** from the **Jobs** top bar menu.

The New Task wizard will be displayed. Enter the required details on each page of the wizard. The new job will be added to the schedule list.

4.6.2.1 Program Title

If the CBMR Scheduler is selected by default, then the following dialogue will be displayed when creating a new scheduled job:



Enter a descriptive name for the job. This name will appear in the job list. Also specify the name of a Backup Selection and the credentials to run the backup job.

4.6.2.2 Program

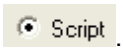
You can choose to run a job with a Backup Selection script file or a command file. CBMR works quite happily with both, so it is a matter of what best suits your way of working.

Type the full path and script name or command file name.

If you are not sure what to enter in this field, use the Find... button to select a script or to locate and specify a command file.

Using a Backup Selection script

Copyright © 1998-2014 Cristie Software Ltd.

To use a script, select the Script radio button 

. Pressing the Find... option displays a list of available scripts.

Using a command file
There are some benefits in using a command file. For example, you could include several scripts which would run one after the other (as opposed to using the script file option where only one job can run at a time).

To use a command file, select the Cmd file radio button

. Pressing the Find... option with the command file option opens the *'Select File To Run'* window. From here, locate the command file and select the Open button.

4.6.2.3 Set Date and Time

In this section of the window you can set when you want the job to run. There are several options you can set here:

- **Weekdays**

Monday to Friday are ticked in the list

- **All days**

Sunday through to Saturday is ticked

- **Weekly basis**

a job can run on a weekly basis. For example, to run a job every Thursday, tick the Thursday box, set the time option and set the Repeat option (box ticked).

- **Monthly basis**

a job can be run on a monthly basis. For example, you could select Monday and Monthly plus the Time setting and set the Repeat option (box ticked). This means that the job would run on the first Monday of the month at the time set. (In actual fact the program runs on the first Monday it encounters. So, if your machine was switched off over the first two weeks of the month, the job would then run on the first Monday encountered after you switch it back on.)

- **Defined date**

a job can be set to run on a particular date. When the **Date** box is ticked press the **Set...** button to display the calendar. Select the date you require, the current date is the default. The arrows at the top of the calendar allow you to change Month and Year.

> changes the month forward **>>** changes the year forward

< changes the month backward **<<** changes the year backward

If the **Repeat** box is checked when a **Date** is set, the date automatically increments to the next day after the job has run.

The **Time** is set by selecting the up/down arrows next to the Hour and Minute boxes.

4.6.2.4 Scheduler Options

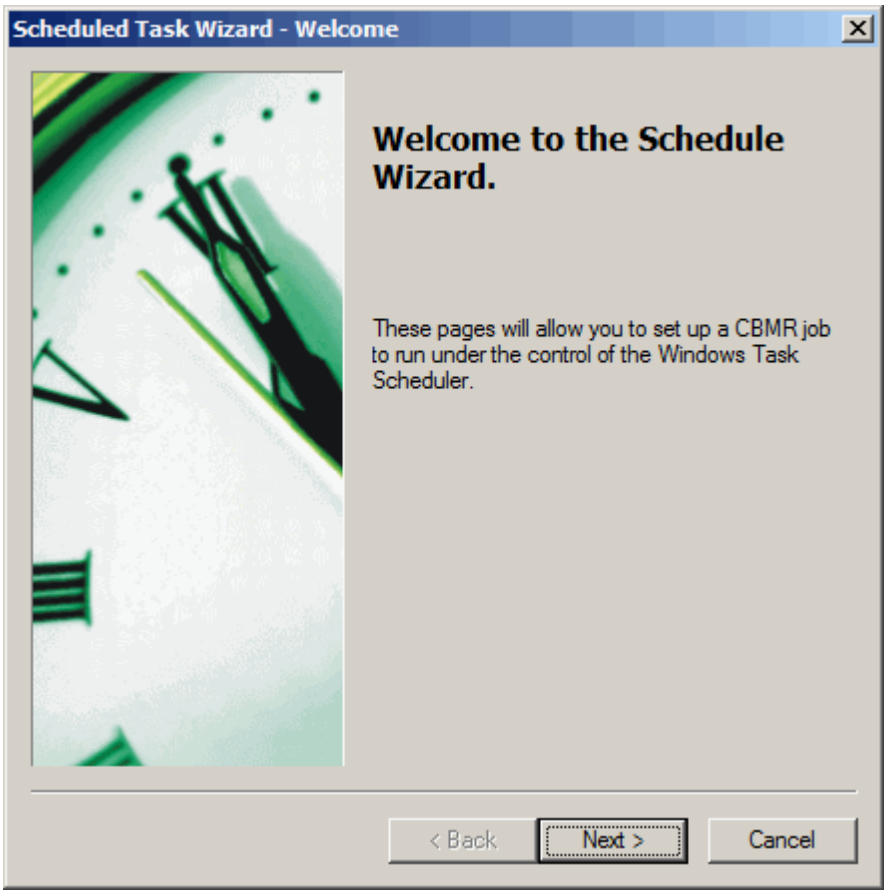
You can run a job on a regular basis by setting the **Repeat** option (the box is ticked when active). When this box is ticked, the job will be repeated until you cancel the **Repeat** option. For example, if a job is scheduled to run on Monday at 8.0am then, with the **Repeat** option set, this job will run every Monday at 8.0am until you cancel the Repeat setting.

If the **Repeat** option is not checked for a particular job, then the job will disappear from the scheduled jobs list after it has run.

Run Detached

You can run a job as a background process while you continue to work in other applications. When the **Run detached** button is ticked, the job will run as a detached process.

4.6.3 Scheduled Task Wizard


Scheduled Task Wizard - Welcome
Welcome to the Schedule Wizard.
These pages will allow you to set up a CBMR job to run under the control of the Windows Task Scheduler.
< Back
Next >
Cancel

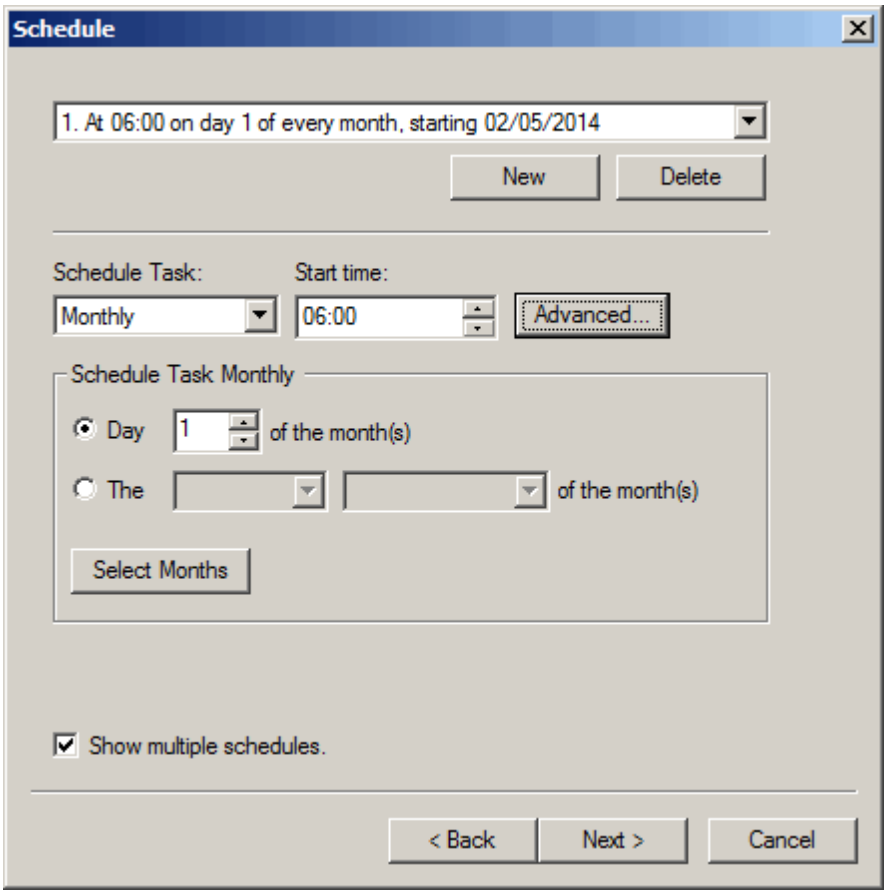
CBMR uses the **Microsoft Windows Task Scheduler** service to schedule unattended backups. The Windows Task Scheduler service allows very flexible schedules to be created.

Creating a new schedule from the Scheduled Tasks tool or from the Backup Selection Script Wizard will start the Scheduled Task Wizard.

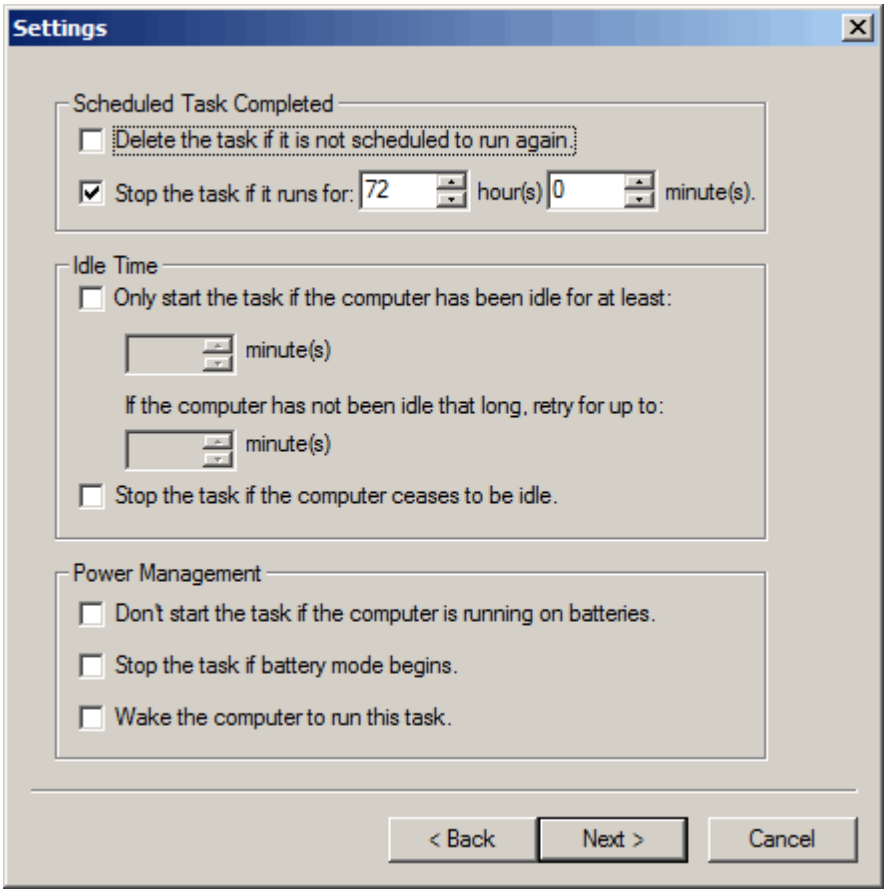
The Scheduled Task Wizard will create a schedule within the Windows Task Scheduler service to run a CBMR backup selections script or a command file. Note that this is entirely independent of the CBMR Scheduler service.

Copyright © 1998-2014 Cristie Software Ltd.

4.6.3.1 Schedule

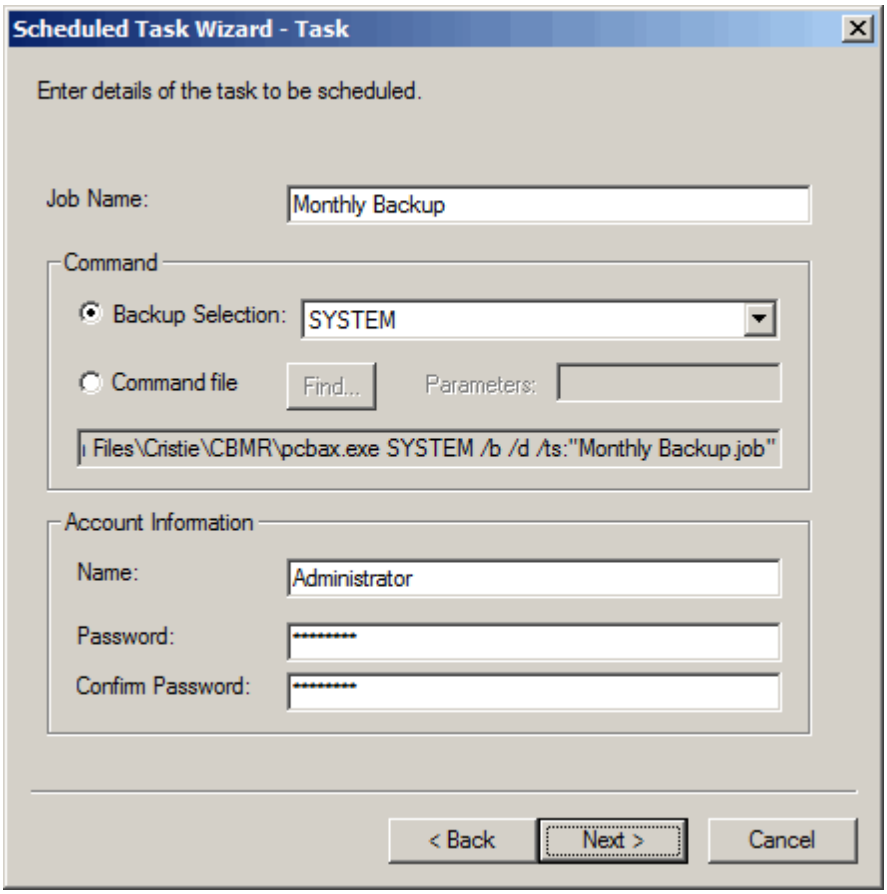


The next two pages of the setup allows the schedule for the job to be defined. The second page allows finer control over the job settings:


Settings
Scheduled Task Completed
Delete the task if it is not scheduled to run again.
Stop the task if it runs for: 72 hour(s) 0 minute(s).
Idle Time
Only start the task if the computer has been idle for at least:
minute(s)
If the computer has not been idle that long, retry for up to:
minute(s)
Stop the task if the computer ceases to be idle.
Power Management
Don't start the task if the computer is running on batteries.
Stop the task if battery mode begins.
Wake the computer to run this task.
< Back
Next >
Cancel

Copyright © 1998-2014 Cristie Software Ltd.

4.6.3.2 Task



The task page allows you to enter details of the command that will be executed.

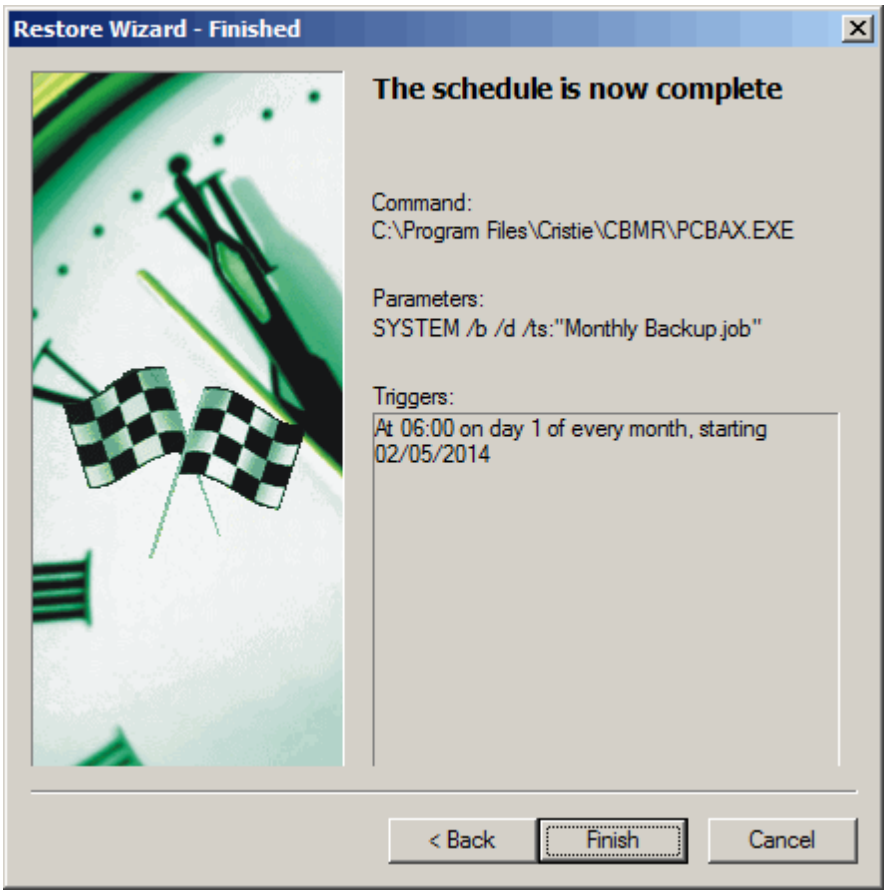
The job title must be a unique string to identify the job. This will be used to create the job file in Windows Task Scheduler.

The command can be an existing CBMR Backup Selection script, selected from the drop-down list, or a command file with parameters. Note that if the Backup Selection Script Wizard has started this Wizard automatically, the command fields will already be filled in and cannot be changed. The actual command that will be run is displayed for information purposes.

The **Account Information** defines the login details under which the command will be run.

The following two pages in the Wizard are provided by the Microsoft Windows Task Scheduler service and provide help through tooltips. They allow you to specify dates, times and frequencies at which the job will be run, and various restrictions concerning power management and how long the task is allowed to execute.

4.6.3.3 Finished



The final page in the wizard summarises the command and the times at which it will be run.

4.6.4 Managing Scheduler Jobs

Attaching/Detaching Jobs

If you want to check on the progress of a scheduled job which is running, selecting the **Attach** option from the **Jobs** top bar menu (or double clicking on the tape icon) will open the Backup Status window.

Pressing the **Detach** button in the status window returns you to the Scheduler jobs window.

Putting a Job on Hold

You may need to hold back a routine backup, for example, people are working late and you don't want the backup to run until everyone has finished with the system.

To put a job on hold:

1. Select one or more jobs in the Scheduled Jobs tool.

2. Select **Hold\Selected** from the **Jobs** top bar menu. You can also apply 'hold' to all jobs by selecting **Hold\All**.

The job(s) will not run until released.

The icon representation will change to identify the status of the job.

If a detailed view of the Scheduled Jobs tool is displayed (**View / Details**), you will see the job

Copyright © 1998-2014 Cristie Software Ltd.

status (**Held, Waiting** or **Running**).

Changing an Existing Job

To change an existing Scheduler job, click on the **Configuration** *Backup Schedules* drop-down menu option.

Then open the job details by double clicking the relevant job or select **Open** from the Jobs top bar menu.

You can then make the appropriate changes to the job details. Press OK to confirm your changes.

Deleting a Job

To delete a scheduled job, select your chosen job from the scheduled jobs list.

Then select **Delete Selected** from the **Jobs** top bar menu. You are prompted to confirm the delete action.

Running a Job Immediately

If you need to run an ad hoc job or test a job you have set up, then select the **Run** option and the job will run straight away. This will not affect any time/date parameters that you have already defined. If you have set the job to run nightly at 10 o'clock, it will still do so.

Releasing a 'Held' Job

In order to release a Held job, select the job(s) that are on hold.

Select **Release\Selected** from the **Jobs** top bar menu. You can also apply *'Release'* to all jobs by selecting **Release\All**.

If you display the detailed view of the Scheduled Jobs tool (**View\Details**), you will be able to view the status of each job in your queue (**Held, Waiting** or **Running**).

4.6.5 System Dependent Information

The Scheduler Service

CBMR can schedule jobs to run with no user interaction. These jobs are configured to be executed by a special type of program known as a **service**. The main reason for this is to allow scheduled backups to run even when a user is not logged on to the system.

What are Windows Services ?

Windows services are a special class of program that are installed and controlled by the Windows Service Manager. The Service Manager can be accessed from the control panel allowing services to be started, stopped and also have their properties modified.

One of the most important points to remember is that services should not, and in most cases cannot, directly interact with the current users console.

Windows Scheduled Tasks Service

Microsoft Windows provides its own scheduling service, called the Windows Task Scheduler. CBMR jobs can be configured to run under the control of the Windows Task Scheduler. They require a Job Name option (**/ts:***JobName*) where JobName is the name of the Windows Task Scheduler job. Again, the CBMR program will automatically add this parameter when scheduling a script.

The Windows Scheduled Task Service allows very flexible schedules to be created.

4.6.6 Using Batch Files

There are many occasions when other operations are required for a backup in addition to the actual backup process itself. For example, copying the log file to a specific location, parsing the log file, e-mailing status etc. When additional commands are required, you can create a batch file to perform the backup job and specify this as the job to be run by the scheduler.

When running a batch file it is important to remember that if you want to attach to a running job to interact with it or view the status, you will need to specify the **/d** option as one of the parameters on the CBMR command line. You must specify the **/ts:task.job** option where **task.job** should be replaced with the name of the Windows Task Scheduler job.

For example, to run a Backup Selection script called *weekly.scp* the following batch file could be used:

```
rem start of batch file
rem other commands can go here
rem remember the /d option to specify detached mode (and, if
rem using the Windows task scheduler, the /ts: option to
rem specify the task this batch file belongs to)!
pcbax weekly /b /d /ts:weekly.job
rem other commands can go here
rem end of batch file
```

> ***Note: if you do not specify the /d option (and, if using the Windows Task Scheduler, /ts: option), or if you run a program other than pcbax.exe then you will not be able to attach to the job to view the status. The scheduler will run the program and will indicate that the program is waiting, running etc. from the job folder but attempting to attach to the job will result in an error indicating that CBMR was unable to attach to the job.***

4.7 Backup Catalogue

A Backup Catalogue has two major advantages:

- It is quick and easy to locate data on a backup
- It allows you to keep more information about a backup than is possible on the backup media, and you have instant access to the contents of the selected volume

Using the Backup Catalogue enables you to view any volume (**Volume** top bar menu) without having to connect a Backup Location or load the media. This can be a considerable time saver if you are searching for a directory or files and you are not sure on which volume they are stored (**Search** top bar menu), especially if you take into account a large organisation where there may be a large number of volumes retained.

The **View** top bar menu provides different display options: Large/Small icons, a List or a Detailed view. The Details View provides some extra information about the volume. It details the volume name, the date/time created, the tape format type (currently SDB) and an ID (this is a number assigned internally to the volume).

The **Sort** top bar menu allows you to arrange the catalogue entries in alphabetic sequence (**Sort by Name**) or in date sequence (**Sort by Date**).

> ***Note: in the Details view you can also click in the relevant column heading to sort the***

Copyright © 1998-2014 Cristie Software Ltd.

entries in Name, Date or Time sequence.

The **New** option allows you to create a catalogue entry. For example, you may have some backup volumes for which no catalogue entry was created at the time of the backup.

The Backup Catalogue appears on the main CBMR Tools menu option.

4.7.1 Viewing the Catalogue Contents

You can access the **Backup Catalogue** contents either by selecting the Backup Catalogue icon or selecting **Restore, Compare** or **Verify** from the CBMR Tools menu and selecting the **Use Backup Catalogue** option.

At this point you have not committed to a particular volume or Backup Location, you are merely viewing the entries in the catalogue listing. Similar to other displays e.g. Backup Location scripts, the view can be as an Icon or a detailed listing (**View** top bar menu). The detail includes Volume name, date and time the backup was created and the format. The **Details** display can be sorted by Name, Date and Time.

4.7.2 Information Stored about the Backup

Each backup is stored as a volume. There is one volume available per media (tape, file etc), Details about the backup volume are stored as the **Media Header**. Access to a volume may be locked with a password

Each drive backed-up within a volume is known as a dataset. Details about the drive are stored as a **Dataset Header**. Access to a dataset may be locked by a password.

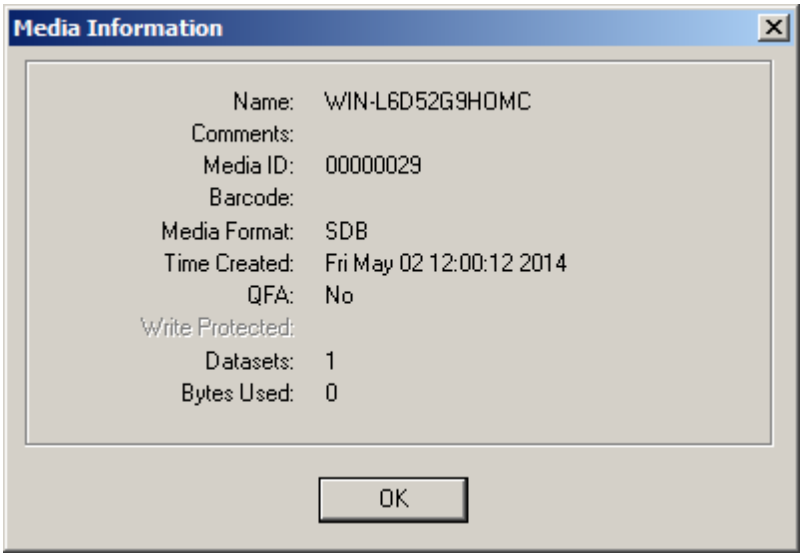
The Media and Dataset headers can be viewed through the **Backup Catalogue**. The amount of information about the files and directories stored within a dataset is defined when the backup is made.

4.7.2.1 Media Header

Note: the Media Header is information written at the beginning of the media, eg. Name, Date and Time created, whether the data is password protected. This information may be useful at a much later date if you are trying to locate a backup.

Select the Media Header... option from the top bar Backup Catalogue **Volume** menu.

The *Media Information* window shows all the available information for the selected volume:



Even if your volume is unnamed you will get other details, such as the date and time created, which may give you a clue as to which volume you need. However, it is recommended that all backups are given a meaningful name which provides an indication to the contents.

Name	User-defined
Comments	User-defined
Media ID	Set by system
Media Format	
Time created	Set by system
QFA	Quick file access. Defined by user at backup. Dependent on media
Write protected	Defined by media
Datasets	Number of datasets within volume
Bytes used	Size of backup in bytes

Please also see the Media Header Overview section for additional details.

> ***Note: Quick File Access (QFA) is a facility on some tape drives which enables rapid access to files during Restore. The tape is divided into two areas: a catalogue area and a data area. The catalogue area at the start of the volume stores directory information which points to the data area where the actual data is stored. During Restore the program locates the file entry in the catalogue and goes straight to the correct point in the data section.***

During backup, the directory catalogue is written first - therefore in a situation where a backup extends over multiple tapes the first tape (containing the directory catalog) must be used to start a Restore.

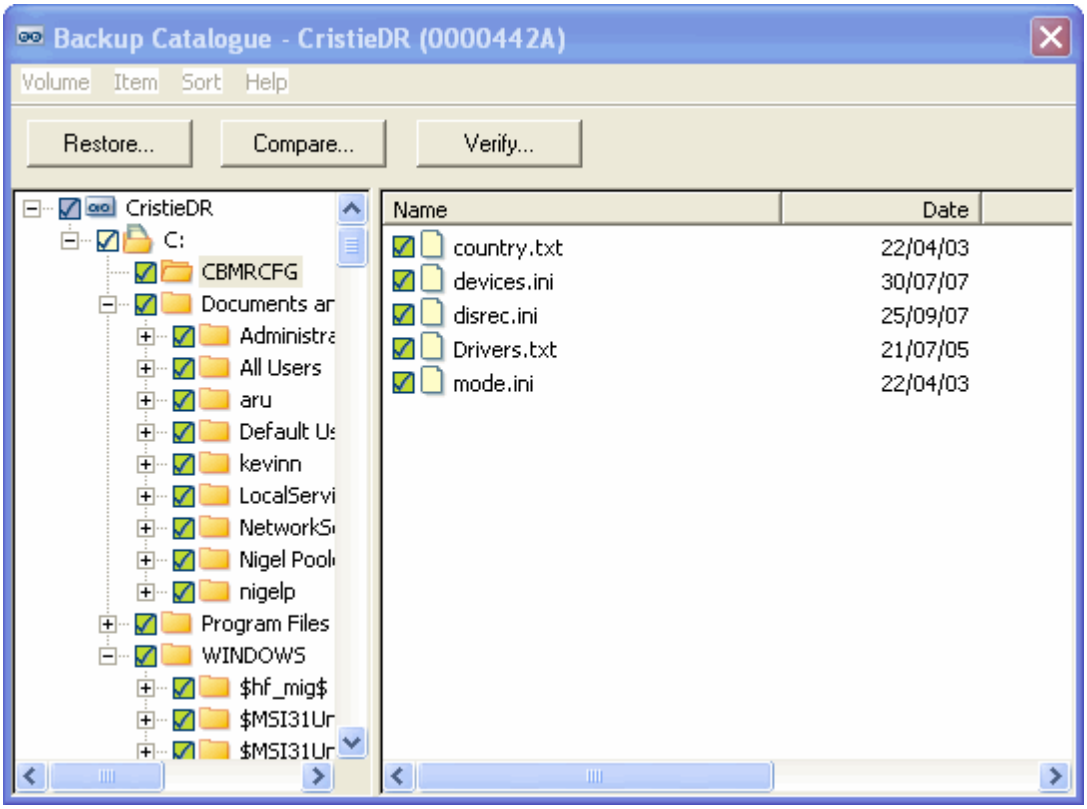
Copyright © 1998-2014 Cristie Software Ltd.

4.7.2.2 Dataset Header

The **Dataset Header...** option in the top bar **Item** menu provides detailed information about the selected dataset. The information should help you identify a backup and decide if it is the one you want.

Name	User-defined
Comments	User-defined
Time created	Set by system
Barcode	(From barcode label on media)
Resource	
Compression	Defined by user at backup
Software version	CBMR software version used to create it
Size	Size of backup in bytes
Catalogue Info level	Set by user at backup
Backup Location	Backup Location holding the backup datasets

4.7.3 Browse Backup Catalogue



The Backup Catalogue browse window is shown when you open a Backup Catalogue volume to select data to be restored, compared or verified. Buttons are provided to begin a restore, compare or verify operation.

It is at this stage that the level of information which you defined at the Backup stage becomes evident (Full, Partial, Brief or None). For example, if you specified 'Full' then media and dataset headers, directory and file information will be available; if you specified 'Partial' there will only be media and dataset headers and directory details. So, if you select a dataset and get the message *'This dataset entry does not contain directory information'* it means that you have specified 'Brief' and only the Media and Dataset headers are available.

If a password was entered when a dataset was created, you will be prompted to enter it when you open the dataset. You must supply the correct password, you cannot over-ride this prompt.

The **Volume** menu provides options to view the **Media Header** for the volume being browsed, change the **Info Level** stored within the volume (this may require the media to be queried), set **Restrictions** on whether the selected data is actually restored, compared or verified, begin a **Restore / Compare / Verify** operation and **Close** the volume.

The Item menu (which is also available as a context menu) provides options to **Tag** or **Untag** the selected item, view the **Dataset Header** for the selected dataset, view a **Selection List** of the items selected from the current dataset, **Redirect** an item to a different location from where it was originally backed up, view a **Redirection List**, and view the **Media Header** for the current volume.

The **Sort** menu is available when at least one item is highlighted in the file list view. It enables the file list to be sorted in a variety of ways. The file list can also be sorted by clicking on the list's column headers.

Copyright © 1998-2014 Cristie Software Ltd.

4.7.4 Modifying the Level of Catalogue Information

You can change the level of information held by the Backup Catalogue. Select the **Change Info Level** option from the top bar **Volume** menu in the Backup Catalogue tool.

The **Current Info Level:** tells you the information level of the selected volume (The 'Current Info Level:' will be 'None' if you are creating a new entry).

If you want to down-grade the level of information, for example from **'Full Information'** to **'Headers and Directories'** or **'Headers Only'**, then just click on the required option. You are given the opportunity to cancel the action.

However, if you are up-grading the information level, then you need the media loaded so that the relevant information can be read from the media and written to the catalogue entry. You will be prompted to select a Backup Location to use. When you select the Backup Location storage device to use for this operation, CBMR checks the location, compares the Media Header with the selected header in the catalogue entry and, if correct, proceeds with the upgrade. You will be prompted to connect the correct location or insert correct volume if either does not agree with your selection.

You are informed when the update is complete.

Select Required Info Level

You can choose to store any one of three levels of information. The current level will be 'None' if this is a new volume or, if you are modifying a Catalogue entry, the existing level will be quoted (which of course could also be 'None' if that is what is defined in the backup selections script).

The levels of information are as follows:

- **Headers Only**

Volume and Dataset headers. This is a minimal level of information and takes up little space

- **Headers and Directories**

Volume, Dataset and Directory details

- **Full Information**

All of the above, plus File information. This will be significantly larger than Brief or Partial entries

4.7.5 Creating a New Catalogue Volume

You can add new volumes to the **Backup Catalogue**. For example, if a backup job specified no entry in the Backup Catalogue at the time it was run, or Backups which were created prior to using CBMR.

CBMR is compatible with Cristie's SDB Backup and Recovery Software.

1. Insert the media into the Backup Location storage device
2. Select **New** from the top bar Backup Catalogue menu
3. You are prompted to select a Backup Location storage device and define the level of information you wish to record
4. Select OK when the operation is complete; the entry is added to the catalogue listing

4.7.6 Deleting, Searching and Restoring

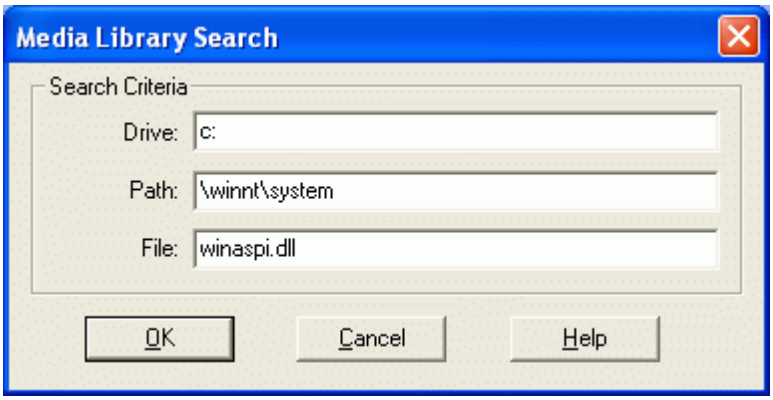
Deleting a Volume From the Catalogue

Select the **Delete Selected Volumes** option from the top bar Backup Catalogue **Volume** menu. You are given the opportunity to cancel the action or to continue. This is only deleting a catalogue entry and has no bearing on the actual data.

Searching the Backup Catalogue

Select the Backup Catalogue top bar **Search** option to display the search menu. You have the option of searching **All Volumes** or **Selected Volumes**. You can make a multiple selection by pressing the shift key while clicking on the each line in turn.

You must provide some parameters to direct the search; how specific you are refines or widens the search field.



If you do not supply a full path, then all occurrences of the search object will be listed in time order with the most recent at the top of the list.

You can search for an individual file but obviously you must have the 'Full' level of information on this volume, otherwise there will be no file details to search.

If you want to locate an individual file, you must enter the full file name, wildcards (E.g. ***. doc**, **pcbax.***) are not accepted.

Restoring Data via the Backup Catalogue

You can initiate a Restore, Compare or Verify operation from the Backup Catalogue Volume window by selecting **Restore / Compare / Verify** from the **Volume** top bar menu or by pressing the appropriate button.

You can also select **Restore, Compare or Verify** from the CBMR Tools menu which will start the Restore/Compare/Verify Wizard. This will give you the option of using the Backup Catalogue or the Backup Location to select the data you are interested in.

4.7.7 Backup Location Search

This window allows you to search the Backup Catalogue.

You can search for an individual file but obviously you must have the 'Full' level of information on this volume, otherwise there will be no file details to search. Wildcards (E.g. ***. doc**, **pcbax.***) are accepted.

If you do not supply a full path, then all occurrences of the search object will be listed in time order, with the most recent at the top of the list.

Copyright © 1998-2014 Cristie Software Ltd.

Backup Location Entry Information

This window displays information about the selected entry resulting from a search operation.

Details about the volume, the dataset and the specific entry are shown. This information is a useful checking option before you actually restore the data.

Backup Location Search Results

This window displays the results of the Search operation. Select **View Information** from the **Options** menu to display detailed information about the selected volume.

When you have found the data you want to restore, you can set the Restore program in action using the **Start** option in the top bar **Options** menu.

4.7.8 Select Backup Location To Use

This window is displayed when you press the 'Select the Location to Use' button when updating the Catalogue information or when you want to create a new entry.

For example, if you are upgrading the catalogue information level, then you need the original data loaded so that the relevant information can be read from the media and written to the catalogue entry. You are prompted to select :

the location used to write the data.

the location defined as the default.

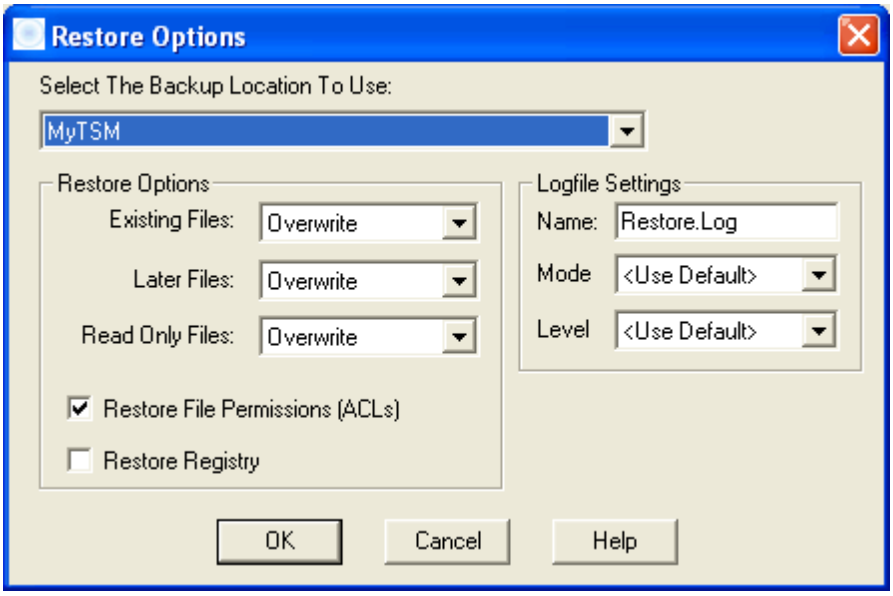
pick one from the list of configured locations.

Both the original Backup Location and the default location will be identified below the relevant buttons.

CBMR now checks the location, compares the media header with the selected header in the catalogue entry and if correct proceeds with the upgrade. You will be prompted to connect the correct location or insert the correct volume if either does not agree with your selection.

If you want to use a location which is not listed, then you need to open the Backup Location menu option and define its properties. See the chapter on Creating a New Catalogue Volume for further details. The new location will be included in the list.

4.7.9 Options (Restore/Compare/Verify)



The title of this window depends on which program you have selected: Restore, Compare or Verify. However, you are not bound by that selection and if you change your mind, for example you decide to compare the data before you restore it, then you can run the Compare program from this window.

You can accept the default settings or you can specify different rules which will only apply to the current job.

> ***Note: any changes made here will not change the values defined in the Default Settings property sheet.***

Select the backup location to use

Select the location from which you are accessing the data. All the configured locations are listed.

Restore Options

- **Existing Files** - if any files being restored already exist on disk then you can direct CBMR to respond in one of the following ways:

- *Skip* any file it encounters which already exists

- *Ask* whether it should overwrite or skip the file

- *Overwrite* the existing file with the file from the backup

- **Later Files** - if any files being restored are found to be later versions than those already existing on disk, then you can direct CBMR to respond in one of the following ways:

- *Skip* any file it encounters which are later versions

- *Ask* whether it should overwrite or skip the file

- *Overwrite* the file on disk with the later version from the backup

- **Read Only Files** - if any read only files are being restored already exist on disk, then you can direct CBMR to respond in one of the following ways:

- *Skip* any read file it encounters which already exists on disk

- *Ask* whether it should overwrite or skip the file

Copyright © 1998-2014 Cristie Software Ltd.

- *Overwrite* the file on disk with the file from the backup

Logfile Settings

Log files are a useful source of information and will list any error messages. Log file information can be important if problems have occurred. The following options are available:

- **Name**

- the default will be the log file of the selected operation (restore.log, compare.log or verify.log). If you have decided to run a different program from the one selected in the Tools menu, for example Compare instead of Restore, then you will have to overtype the default entry with the log file name relevant to the operation

- **Mode - Overwrite/Append**

- if *Overwrite* is set, then each time the log file is created it overwrites the existing one

- if *Append* is set, then each log file is appended to the previous one

- **Info Level - Full/Partial/Brief/None**

- a *Full* logfile contains a list of all files, errors (if any) and statistics

- a *Partial* log file contains sub-directories, errors (if any) and statistics

- a *Brief* log file contains errors (if any) and statistics

- if *None* is selected, then no log file is created

Restore Security Info - (Windows NT installations only)

Select this option (ticked) if you want to restore the security information associated with the directory. If the option is not ticked, then only the data is included

> ***Note: you must be logged on the computer as a user account with the appropriate rights to restore security data***

Restore Registry

Select this option if you want to restore the Registry files. You must reboot your system after restoring the registry files.

4.8 Backup Strategy

Backing up data to a data cartridge is a convenient and secure means of ensuring vital information can be retrieved in the event of a disaster. A disaster in this instance does not necessarily mean a major earthquake or such like. Loss of data can be due to relatively common occurrences like accidental deletion, data corruption, software/hardware failure, power failure (even minimal) or theft of equipment. If you consider the effect of losing a complete weeks data, or even a day or two, then you can appreciate the importance of backing up your data. Also, most companies are legally required to keep data for a period of years and therefore an efficient archive and retrieval procedure releases expensive hard disk space for working data.

The backup routine you employ depends on several factors: how often does the data change, how valuable is the data (time and money invested in it), how much time can be allotted to carrying out the backup. Remember that the scheduling option in CBMR provides for unattended backups. There are several established backup strategies and you can use the one which suits your working practices best or use one as a basis for developing your own pattern.

Points to Consider:

- Identify the backup needs of your company and create a suitable backup regime
- Once established maintain the routine (Make use of the CBMR automated routines)
- Identify the backups with meaningful titles so that you can restore your files quickly and with the appropriate version of the data
- Follow the maintenance procedures for your tapes and drive (tape storage, drive head cleaning etc)
- Store tapes in a secure location and maintain copies off-site in case of theft, fire or flood damage

4.8.1 Example Routines

If you maintain efficient backup procedures, you should always be able to recover any lost data with minimum effort - whether it is due to external causes, a fatal malfunction during a backup or just a routine retrieval of archived data. Always use meaningful descriptive labels so that tapes can be identified quickly and without confusion ('Fred's Backup' may not be very helpful when the system has crashed and an entire department want their data restored asap!)

There are three typical Backup routines described here, but ultimately you need to instigate a routine which best suits your company requirements.

For specialist advice on backup strategies and how best to secure your data, please contact Cristie Software Limited.

Three Week Backup Cycle

The most basic backup provides three weeks of data.

On the first working day of the week, a complete backup of all files is carried out. On subsequent days of the working week, newly-created files and modified files are backed up.

This procedure is followed for three weeks. On the fourth week, the first weeks tapes are re-used, then the second weeks and so on, in a continual cycle.

Reasonably small computer systems would allow the one full backup and four partial backups to be stored on one volume, therefore only requiring three volumes.

Twelve Week Backup Cycle

This backup regime allows you to recover data from up to twelve weeks ago. This pattern is more suitable for larger systems, systems where there are frequent file changes, or systems which require a longer data history.

Volumes should be labelled as follows:

Monday, Tuesday, Wednesday, Thursday

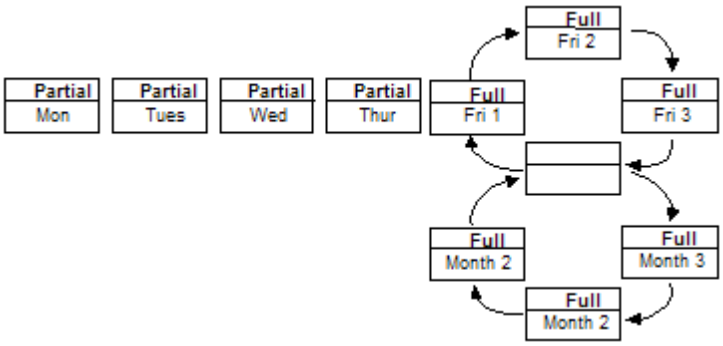
Friday 1, Friday 2, Friday 3

Month 1, Month 2, Month 3

The Friday 1-3 and Month 1-3 volumes are used for full backups, the others for partial backups (new and modified files only). 'Month' is not strictly accurate; the volumes are used every four weeks.

The following diagram illustrates how the tapes are used:

Copyright © 1998-2014 Cristie Software Ltd.



Again, depending on the amount of date to be backed up, this method can use as little as ten volumes.

Three Year Archive

This is a comprehensive Backup cycle which will provide three years of data. A time span of this nature must be considered where legal requirement calls for data to be kept for a number of years, for example accounts information.

Each year, a full backup is taken of all data and archived.

Each month, a full backup is taken. The monthly tapes are re-used on the corresponding month of the following year.

A weekly backup is taken on an appointed day each week (typically the first working day). The weekly tapes are re-used on the corresponding weeks of the following month. (Again, the month is regarded as a four week cycle.)

Daily backups are taken and the tapes reused on corresponding days the following week.

The monthly, weekly and daily tapes should be kept in a fireproof safe. The yearly backup should be stored off-site.

You now have substantial coverage should you need to recover data. There is data for each individual day plus weekly and monthly and annual backups.

4.9 Running CBMR from the Command-line

CBMR can be run as a console based application using the program **pcbax.exe**. (PC-BaX)

In a command window, change the directory to where CBMR is located.

At the prompt, type: **pcbax /?** for a list of commands and description of usage.

Usage:

pcbax <script> <mode>[options] ....<script> (omit the **.scp** extension) is any Backup Selection script contained in the **\pcbax\scripts** directory
pcbax /ds:n [options] .... restores all files in dataset *n* where *n* is the number of the dataset. The first dataset is 0 and is the default if a number is not supplied. For example: **pcbax /ds:2** restores the files in the **third** dataset.

This provides a quick way to restore all the files within a dataset without needing to specify a Backup Selection script.

pcbax /cl:<media name> ....checks that the correct media is loaded in the Backup Location.

pcbax /cw .....checks if the media is write protected.

pcbax [<script>] /cmh .....creates a new header.

pcbax /sms .....shows media status.

pcbax /smh .....shows media header

<Modes> are:

/b Backup

/r Restore

/c Compare

/v Verify

[options] are:

/sd: <*device*> Where *device* is the name of the Backup Location storage device you wish to use to override the default location OR the location specified in the Backup Selections script

/h Disables screen output

/s shows statistics during backup in place of file names

/p:<media password> This password overrides any script specified password

/unload Unloads media at end of operation

/registry Replaces registry files if found during restore

/erase Performs a security erase on the media

/retension Performs a retension operation on the supported location/media

/initialise Performs a partition operation on the supported location/media

4.9.1 PC-BaX Command Line Options

CBMR can be run as a console based application using the program **pcbax.exe**.

In a command window, change the directory to where CBMR is located.

At the prompt, type: **pcbax /?** for a list of commands and description of usage.

Usage:

pcbax <script> <mode>[options] ....<script> (omit the **.scp** extension) is any Backup Selection script contained in the **\pcbax\scripts** directory

pcbax /ds:n [options] .... restores all files in dataset *n* where *n* is the number of the dataset. The first dataset is 0 and is the default if a number is not supplied. For example: **pcbax /ds:2** restores the files in the **third** dataset.

This provides a quick way to restore all the files within a dataset without needing to specify a Backup Selection script.

pcbax /cl:<media name> ....checks that the correct media is loaded in the Backup Location.

pcbax /cw .....checks if the media is write protected.

pcbax [<script>] /cmh .....creates a new header.

pcbax /sms .....shows media status.

pcbax /smh .....shows media header

pcbax [<script>] /scan .....scan media into library

<Modes> are:

/b Backup

Copyright © 1998-2014 Cristie Software Ltd.

/r Restore

/c Compare

/v Verify

[options] are:

/sd: <*device*> Where *device* is the name of the Backup Location storage device you wish to use to override the default location OR the location specified in the Backup Selections script.

/ver:<date> The backup version as of <date> to use where <date> should be in the form "DD/MM/YYYY-HH:MM:SS".

/h[s][q] Disables screen output except [s] - always show stats and [q] always show questions. If questions arise and /h is in effect, a USER ABORT is assumed.

/s shows statistics during backup in place of file names.

/p:<media password> This password overrides any script specified password.

/unload Unloads media at end of operation.

/registry Replaces registry files if found during restore.

/erase Performs a security erase on the media.

/retension Performs a retension operation on the supported location/media.

/initialise Performs a partition operation on the supported location/media.

/ts:<ScheduleName> identifies the Windows Scheduler task. If CBMR is being run from the Windows Scheduler, as opposed to the CBMRScheduler Service, then this parameter is required to enable the CBMR graphical user interface to communicate with the scheduled job while it is running. <ScheduleName> must be replaced with the exact name of the Windows Scheduler job (including the .job extension).

/epass:<encryption passphrase> Specifies the encryption passphrase

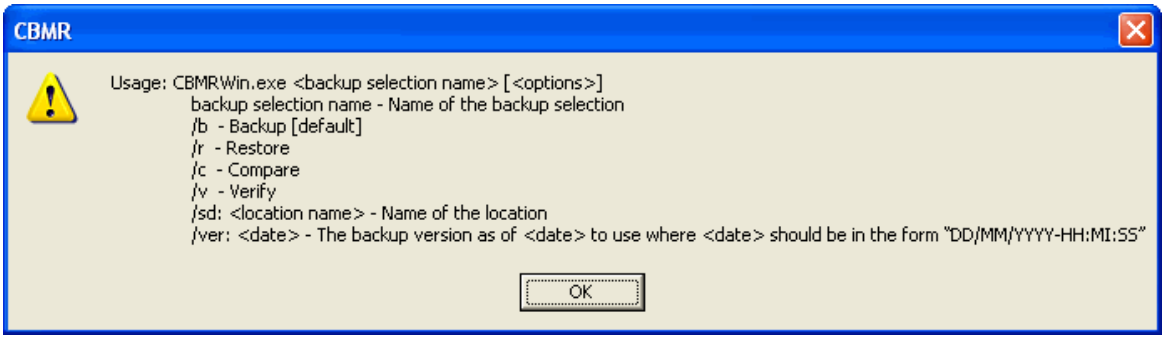
/ekey:<encryption clear key> Specifies the encryption key

4.9.2 CBMRwin.exe Command Line Options

CBMRwin.exe is the graphical based application. You can run some command line options with the GUI version.

In a command window, change the directory to where CBMR is located.

At the prompt, type: **CBMRwin /?** for a list of commands and description of usage.



4.9.3 CBMRCfg.exe Command Line Options

This program allows the system configuration to be created on the command line.

In a command window, change the directory to where CBMR is located.

At the prompt, type: **CBMRcfg.exe /?** for a list of commands and description of usage.

Usage:

CBMRCFG.EXE [options]

Options are:

/help or **/?** - Show usage

/sd {device} - Use device specified instead of the default device

/out {backup|<valid local or UNC path>} - Store configuration in this location

backup - Store the configuration with the backup

/volatile - Do not remember the changes. Changes will be remembered

by default

/scripts - Creates the scripts DISREC.SCP and DISREST.SCP

Existing scripts will be always overwritten!

Information required to access the configuration share

/cfguser <login ID> - Enter as Domain\Username

/cfgpwd <password> - Password

Information required to access a file device

/devuser <login ID> - Enter as Domain\Username

/devpwd <password> - Password

4.9.4 CBMR Configuration Files

The following configuration files are used by the CBMR software. This is not a comprehensive list.

4.9.4.1 PCBAX.INI

This file contains the name of the default **Backup Manager** to connect to (currently this can only be the local one). Also in this file are options to select the preferred user level (0 or 1) and options to disable any of the objects in the main container window.

4.9.4.2 CBM.INI

This file contains the default settings for the **Backup Manager**. These settings are maintained by the **CBMR**Win.exe program. The settings in this file are used by the **CBMRWin.exe** and **pcbax.exe** programs for Backup/Restore/Compare/Compare and Verify operations.

Copyright © 1998-2014 Cristie Software Ltd.

4.9.4.3 USERSHAR.INI

This is an editable text file and is used to define user defined shares.

4.9.4.4 USERINFO.INI

This is an encrypted file containing user names and passwords.

4.9.4.5 DTEXC.INI

This is an editable text file which may be used to exclude any desktop resource by name.

4.9.4.6 KEYREPOSITORY.INI

This is a text file which contains encryption key information.Please do not edit!

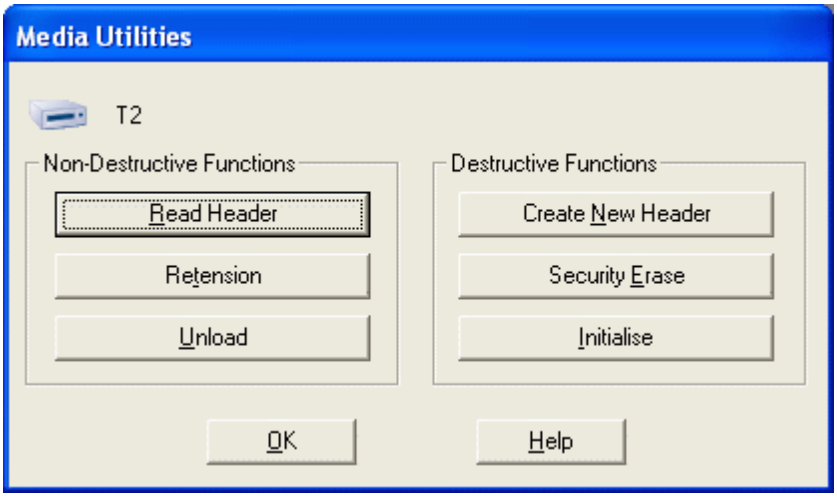
4.10 Media Utilities

CBMR provides a number of media maintenance utilities such as retensioning, initialising or erasing a tape.

Not all options are applicable to every Backup Location type - a message will be displayed if you select an option which is not relevant to the connected location.

Select the *Backup Locations* option from the **Configuration** drop down menu option in the CBMR main menu. Right-click on the **Backup Location** and select **Media Utilities...**

4.10.1 Media Management



The utilities in this window allow you to carry out maintenance tasks on the media. The utilities are divided into **Non-Destructive** and **Destructive** functions.

- The non-destructive functions do not have any affect on the data stored on the media

- The destructive functions will destroy any data currently stored on the media

The connected location is identified in the top left hand corner of the window.

Non Destructive Functions

Read Header	CBMR scans the media and displays the header information
Retension	Removes any slackness in the tape by fast forwarding to the end and rewinding back to the beginning
Unload	Causes the media to be ejected when the backup is complete. Only applies to 'soft load' locations

Destructive Functions

Create New Header	Currently creates a new media header for the volume currently loaded in the location. All existing data will be lost
Security Erase	Completely and irrevocably erase all data from the tape
Initialise	Initialise prompts for a new media header and, as far as the software is concerned, this is now a new piece of media. This option only applies to DAT tapes and you will be advised of this this if you use it on other formats

4.10.2 Read Header

CBMR scans the media loaded in the connected Backup Location and displays the header information which was recorded during Backup. The information is for viewing only; you cannot add, delete or change any details.

4.10.3 Retension

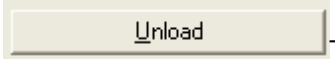
This option is only applicable to magnetic tape media. When a tape is retensioned it simply means that it is wound from end to end and back to the beginning again in order to remove any slackness in the tape and ensures that it is evenly wound on the spool and will feed past the read and write heads smoothly.

A tape should be retensioned:

If it is new - this will ensure that any loose particles left from the manufacturing process are dislodged

If it is left in storage for a period of time - when a tape is not used for a long time there is the possibility of print-through, which means that the magnetic orientation of particles on one layer of tape affect those on the adjacent layer. This can cause data corruption.

4.10.4 Unload



This option will eject the media from all 'soft load' Backup Locations such as DAT drives.

Copyright © 1998-2014 Cristie Software Ltd.

4.10.5 Create New Header

This option will allow you to create a new media header for the media currently loaded in the Backup Location. You can use this option to remove or change a password protected backup.

4.10.6 New Media Header

This window allows you to create a new Media Header for the media currently stored in the **Backup Location**.

Name - Enter a meaningful name which identifies the volume contents

Comments - This field allows you to provide more information about the volume. It is not essential but can be useful if you are viewing a volume at a later date

Password - A password will secure the volume against unauthorised access. Make sure it is a password you will remember at a later date because there is no by-pass procedure and the data will be unrecoverable if you cannot remember what the password is

You have the opportunity to **Cancel** this operation if you change your mind.

4.10.7 Security Erase

Only use this option if you want to totally and irrevocably erase all data from the media. This may be required if the media contained highly sensitive information. This operation takes a considerable length of time to complete, especially for high capacity media because data is erased byte by byte.

4.10.8 Initialise

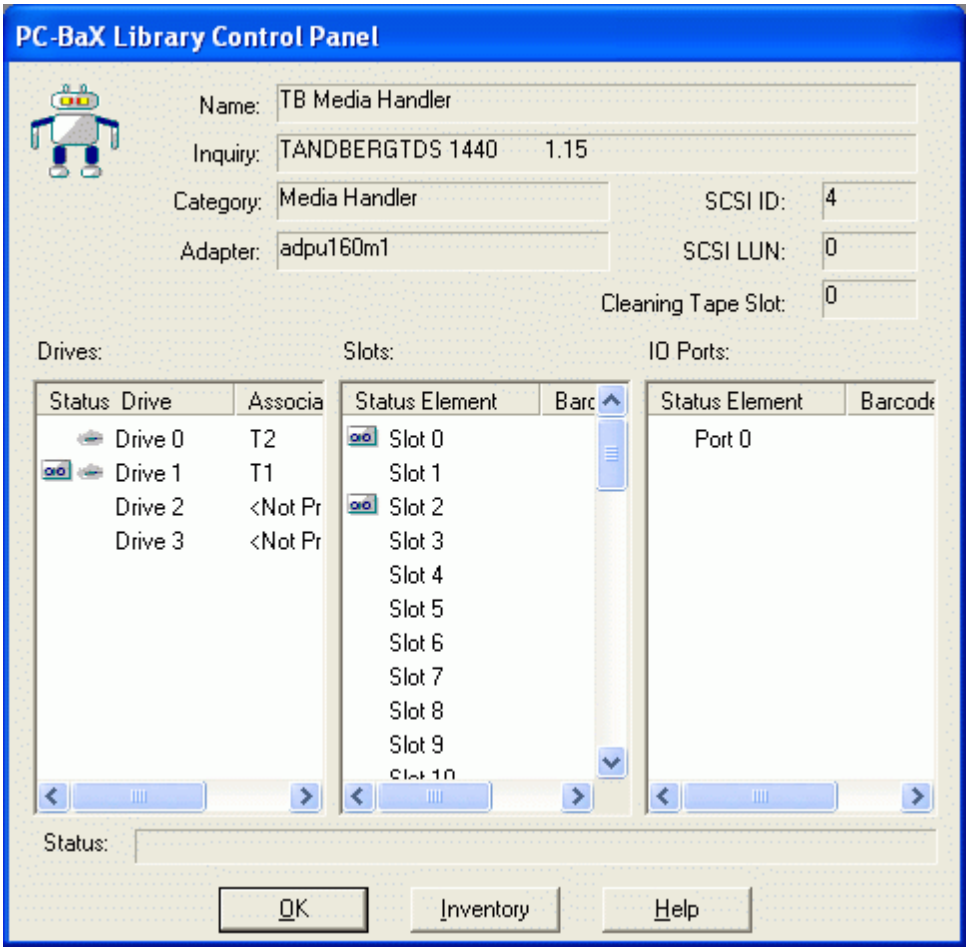
This option only applies to DAT tapes. You will be advised of this if you try to run it on other media types. When you initialise media, you are prompted to enter a media header name and as far as the software is concerned this is now a new, blank piece of media.

You can use the Initialise utility to re-use old media where the stored data is no longer required.

4.10.9 Library Control Panel

CBMR Library Control Panel is an advanced utility for the tape library. Contrary to the notion of associating one drive for every logical library configuration, it is possible to work with the library as a whole and it gives a birds-eye view of the total inventory. If the media are fitted with barcodes and the library is capable of reading them, you will know exactly where each media is. It is also possible to import and export media on the fly, without even opening the library door!

This can be invoked by selecting the **Media Utilities** menu option for a **Media Handler** device.



The presence of a tape icon in the drive status indicates that there is a media in that location.

The Media Handler/Robotics device must have been configured earlier, i.e. SCSI devices are associated with its drives.

Importing Media

To import media to an empty slot or an empty drive, click an IO port slot using the left mouse button and drag it to the desired drive, holding the left mouse button. The valid locations which can accept a media will be highlighted automatically. Once you have highlighted the desired drive or slot, release the left mouse button.

If there is already a media in the IO port it will be moved to the specified drive or slot. If there is no media in the IO port, it will be extended and wait for a media to be placed. The default timeout is 20 seconds. Once a media is placed, it will be moved to the specified location. An inventory will be performed.

Exporting Media

Media from drives and slots can be exported by dragging them and dropping in one of the IO ports. The IO port will be extended and wait for about 20 seconds. After that the IO port will be retracted and an inventory will be done.

Inventory

An inventory can be done by pressing the **[Inventory]** button. After an inventory operation, the drives, slots and IO ports on screen will reflect the exact status as seen by CBMR.

Copyright © 1998-2014 Cristie Software Ltd.

5 Appendicies

5.1 Windows 8 Storage Space and 2012 Storage Pool Support

On Windows 2012, Windows 2012 R2, Windows 8 and Windows 8.1 based systems that are utilising the Storage Pool/Space feature, CBMR will support the backup of the Storage Pool/Space in a passive manner.

This is achieved by storing all the data contained on the Storage Pool/Space as a single volume, that will then be stored in the backup location, during the process of performing your backup. The actual physical construction of the storage pool/space will not be retained in this process.

The process required to protect the data contained on a Storage Pool/Space will typically consist of the following steps:

1. Create a CBMR backup of the system. (This consists of the local partitions, storage pools and the System State)

2. Recover the backup using the CBMR recovery media, choosing just to recover just the Operating System and associated System State.

3. Reboot the recovered system.

> ***Note: When recovering to the original machine, the Storage Pool/Space should still be available. This enables step 4 below to be skipped.***

4. Open Server Manager (Windows 2012/2012 R2) or Control Panel (Windows 8/8.1) and create a Storage Pool/Space. (This does not need to be a replica of the original Storage Pool/Space).

5. Launch CBMR and recover the data from the backup location to an available Storage Pool/Space.

5.2 uEFI and MBR BIOS support

> ***Note: No support is provided for conversion from uEFI to MBR BIOS or from MBR BIOS to uEFI.***

The recovery ISO is not uEFI enabled. Therefore a successful recovery requires a uEFI environment capable of booting the recovery ISO in MBR BIOS.

Physical machines

There are no special considerations that need to be made by the customer for physical uEFI machines.

All Cristie Bare Metal Recovery software handles the recreation of the uEFI and MSR partitions during the recovery of the physical machine, this is transparent to the user. When recovering a uEFI enabled OS you must recover to uEFI capable hardware.

Virtual machines

> ***Important note: When using virtualisation software check the virtualisation software documentation to determine if uEFI is supported.***

To recover to uEFI take the following steps:

1. Once you have a “Recovery Success” message from the CBMR recovery, click Reboot, and then shutdown the recovered VM.

2. Edit the Options of the Virtual Machine, and change the BIOS to be uEFI (instead of the standard MBR BIOS).

3. Once the BIOS has been changed, you will need to boot the VM into the uEFI BIOS using the VM boot options.

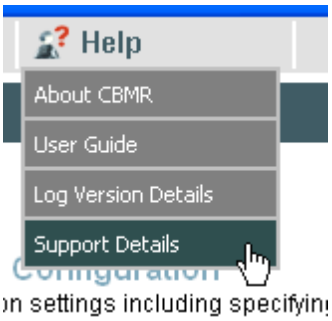
4. When recovery is to a different machine, you may need to configure the uEFI boot Stanza in order to boot the recovered uEFI OS. Please refer to the Cristie Knowledgebase for further information on editing the boot Stanza. This consideration applies to Physical and Virtual recoveries.

Once the above steps have been performed, your recovered uEFI OS will boot in your virtualisation software.

Copyright © 1998-2014 Cristie Software Ltd.

6 Support

Click on the **Help** drop-down menu and select Support Details to display the contact numbers for **Cristie Software** should you have any enquiries or need help with your CBMR package.



Selecting **Support Details** displays a text document called **support.txt** (located in **C:\Program Files\Cristie\CBMR**), which you can change to suit your own requirements. For example, you could edit the file to display your company's technical support contacts.

6.1 Online Help

CBMR includes a comprehensive online Help facility.

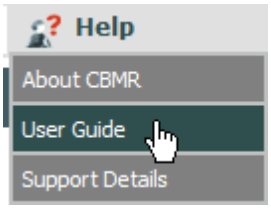
Help is available:

- from the Help push button

- using the F1 key. Help information is displayed for the currently selected operation.
- from the Help top bar menu.
- using the Table of Contents, Index or the Search facility to locate the topic you are interested in.

If your query cannot be resolved through the Online Help Guide, or if you are experiencing problems with your CBMR installation, then please contact Cristie Software's Technical Support team.

To display the CBMR User Guide, click on the Help drop-down menu and select **User Guide**.



This will display the contents of the User Guide.

6.2 Technical Support

The **Support** window lists the contact numbers for Cristie Software Limited.

If you have any queries or problems concerning your Cristie Bare Machine Recovery product, please contact **Cristie Technical Support**. To assist us in helping with your enquiry, make sure you have the following information available for the person dealing with your call:

- CBMR Version Number
- Installed OS type and version
- Any error message information (if appropriate)
- Description of when the error occurs
- All Cristie log files relating to the source or recovery machine. This is very important to help us provide a quick diagnosis of your problem

Contact Numbers - Cristie Software (UK) Limited

Technical Support	+44 (0) 1453 847 009
Toll-Free US Number	1-866-TEC-CBMR (1-866-832-2267)
Sales Enquiries	+44 (0) 1453 847 000
Email	cbmr@cristie.com
Web	www.cristie.com

Support Hours

05:00 to 17:00 Eastern Standard Time (EST) Monday to Friday

Out-of-Hours support available to customers with a valid Support Agreement - Severity 1 issues* only

UK Bank Holidays** classed as Out-of-Hours - Severity 1 issues only.

Severity 1 issues are defined as: a production server failure, cannot perform recovery or actual loss of data occurring.

****For details on dates of UK Bank Holidays, please see www.cristie.com/support/***

Cristie Software Limited are continually expanding their product range in line with the latest technologies. Please contact the **Cristie Sales Office** for the latest product range. Should you have specific requirements for data storage and backup devices, then Cristie's product specialists can provide expert advice for a solution to suit your needs.

Copyright © 1998-2014 Cristie Software Ltd.

7 Glossary of Terms

Adapter definition

An adapter is required to provide a connection between the computer and the device. This may be the parallel adapter which normally connects the printer to the computer, in which case the printer is attached to the back of the drive. Alternatively, the drive may be connected to an adapter card or ASPI

Archive bit

The archive bit is automatically set by the operating system whenever a file is created or modified. If the 'Reset Archive Bit' option is enabled then the flag is cleared when the file is backed up. It will be set again by the operating system when the file is next modified.

ASPI

ASPI (Advanced SCSI Programming Interface) is a standard SCSI software interface linking host adapters to SCSI device drivers. ASPI allows multiple devices to be connected to the one host adapter. This keeps costs down and frees up internal slots.

CBMR

The **Cristie Bare Machine Recovery** product. Enables a disaster recovery of a system from a special minimal backup in conjunction with a DR configuration file held within the backup itself.

Compression

Almost all data exhibits redundancy in the form of repetition. Redundancy of this sort when transferring data is purely wasteful. Data compression is a means of reducing this waste.

Data compression allows the drive to store more data on the same length of tape. In ideal conditions the ratio can be as much as 2:1 or higher.

Data compression also aids performance in that it allows the drive to match the performance of higher transfer rate systems more closely.

Data compression can be performed in 2 ways.

Hardware compression is performed by the backup hardware. This takes the load off the PC but still requires the whole uncompressed data to be transferred over the interface to the backup location.

Software compression is performed by the PC before sending the data to the backup location. This puts extra overhead on the PC in order to compress the data, but it provides less data be transferred over the interface to the backup location.

Dataset header

Each drive backed up is contained in its own dataset on the backup media. The dataset header is information written at the beginning of the backup.

Driver

A device driver is a program which allows a device to communicate with the operating system. Each device must have the correct driver installed to allow the device to operate.

Domains

In the Windows NT environment a domain is a collection of computers which share a common domain database and security policy. The domain name is a unique name by which the domain is known to the network.

DR (Disaster Recovery)

A reference to Disaster Recovery. Also considered to be an abbreviation for the Cristie Disaster Recovery software.

Media header

Information written at the beginning of the media. E.g. Name, Date and Time created, whether the data is password protected. This information may be useful at a much later date if you are trying to locate a backup.

Open File Module (OFM) for CBMR

For Windows 2000 systems, OFM (Open File Module) allows for the safe backup of files that are used by other applications like email and database servers. On Windows 2000 CBMR includes OFM by default and no additional configuration is necessary for this. For Windows XP/2003/Vista systems, the VSS open file manager is used instead. VSS is provided by Microsoft as an integral part of these Operating Systems.

PC-BaX

The Backup and Recovery Software from Cristie, which forms the backup/restore engine of CBMR.

QFA

Quick File Access (QFA) is a facility on some tape drives which enables rapid access to files during Restore. The tape is divided into two areas: a catalogue area and a data area. The catalogue area at the start of the volume stores directory information which points to the data area where the actual data is stored. During Restore the program locates the file entry in the catalog and goes straight to the correct point in the data section.

During backup, the directory catalogue is written first. Therefore in a situation where a backup extends over multiple tapes, the first tape (containing the directory catalogue) must be used to start a Restore.

SCSI ID

Each SCSI device on the chain must have a unique address which the system uses to communicate with that device. The address is represented by the SCSI ID number. The SCSI ID also determines priority when two or more devices attempt to use the bus at the same time.

Volume Shadow Copy Service (VSS)

The Volume Shadow Copy Service provides the backup infrastructure for the Microsoft Windows XP, Server 2003 and Vista operating systems, as well as a mechanism for creating consistent point-in-time copies of data known as shadow copies. CBMR makes use of this technology.

Windows Pre-Installation Environment (WinPE)

Copyright © 1998-2014 Cristie Software Ltd.

The Microsoft Windows Pre-installation Environment (Windows PE or WinPE) is a powerful replacement for the Microsoft MS-DOS operating system in OS deployment processes, test and diagnostic tools development, and system recovery processes. Windows PE is a minimal Windows system that provides limited services based on the Windows XP Professional and the Windows Server 2003 kernels. It also provides the minimal set of features required to run Windows Setup, access and install operating systems from the network, script basic repetitive tasks, and validate hardware.

Cristie is fully licensed by Microsoft to deploy its DR console software based upon Windows PE.